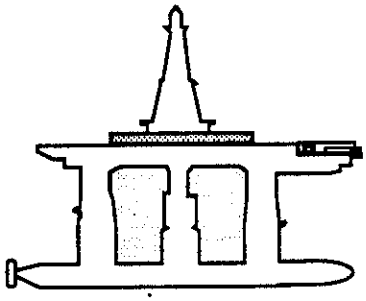
MANAGEMENT OF HUMAN ERROR IN OPERATIONS OF MARINE SYSTEMS



Final Joint Industry Project Report

by

William H. Moore, Dr. Eng.

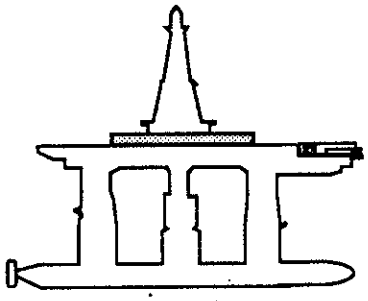
and

Professor Robert G. Bea

Report No. HOE-93-1
December, 1993

Department of Naval Architecture & Offshore Engineering
University of California at Berkeley

MANAGEMENT OF HUMAN ERROR IN OPERATIONS OF MARINE SYSTEMS



Final Joint Industry Project Report

by

William H. Moore, Dr. Eng.

and

Professor Robert G. Bea

Report No. HOE-93-1
December, 1993

Department of Naval Architecture & Offshore Engineering
University of California at Berkeley

MANAGEMENT OF HUMAN ERROR IN OPERATIONS OF MARINE SYSTEMS

Joint Industry Project
Final Report

by

William H. Moore, Dr. Eng.
Marine Systems Engineer
Department of Naval Architecture & Offshore Engineering
University of California at Berkeley

Robert G. Bea
Professor
Department of Naval Architecture & Offshore Engineering
and Civil Engineering
University of California at Berkeley

December, 1993

This report is funded in part by a grant form the National Sea Grant College Program, National Oceanic and Atmospheric Administration, Department of Commerce, under grant number NA89AA-D-SG138, project number R/OE-17 through the California Sea Grant College, and in part by the California State Resources Agency. The views expressed herein are those of the authors and do not necessarily reflect the views of NOAA or any of its sub-agencies. The U.S. Government is authorized to reproduce and distribute for government purposes.

This work also has been sponsored in part by Chevron Research & Technology Company and Chevron Shipping Company, Amoco Production Company and Amoco Transport Company, Unocal Corporation, the California State Lands Commission, the U.S. Coast Guard, the U.S. Minerals Management Service, and the American Bureau of Shipping. The support and guidance of these sponsors is gratefully acknowledged.

We also wish to thank Professor Karlene Roberts of the Haas School of Business at the University of California at Berkeley, Professor Elisabeth Paté-Cornell from the Industrial Engineering and Engineering Management Department at Stanford University, Professor Martha Grabowski of the Rensselaer Polytechnical Institute, and Professor Emeritus Edward Wenk of the University of Washington at Seattle for their valuable insight to the difficult problems of human and organizational error in marine systems.

PREFACE

Catastrophic accidents are not new to the marine industry. However in wake of the large human, environmental, and economic losses in accidents such as the *Exxon Valdez* and *Piper Alpha* disasters, we have begun to address the primary contributing factor to these disasters: human errors. Approximately 65% of high consequence marine disasters are the result of human and organizational errors in operations. At the beginning of this research in 1990, there were no structured quantitative methods to assist engineers in identifying and evaluating strategies to prevent and/or mitigate the effects of human and organizational errors.

As this report develops it will be apparent that there are three major players in the human and organizational error reliability problem: (1) humans (individuals), (2) organizations (groups of individuals), and (3) systems (structures and equipment). The second apparent observation will be that there are two approaches to the evaluation and management of human and organizational errors in improving reliability: qualitative and quantitative. Both of these approaches have benefits. Qualitative modeling forms the basis from which to address the problem through operational procedures and regulation, and quantitative methods provide a means from which the effectiveness of procedures and regulations can be evaluated. This work indicates that they both should be mobilized to identify how and where to improve human and organizational error management. One approach is not a substitute for the other.

The third observation will be the complexity of the problems of interactions between humans, organizations, and systems; this is not a simple problem. Currently, there is little definitive data to assist one in evaluating or analyzing such problems.

The objective of the quantitative analysis developed in this report is not to produce numbers; it is to produce insights that can assist in improving the reliability of marine systems. The quantitative assessments should be used as a decision support tool for qualitative judgments and are not a replacement for sound judgment and common sense.

The intended audience for this report are operators, managers, engineers, and regulators of marine systems. Each has a unique set of experiences that can only serve to enhance the knowledge of the systems being modeled. We trust that this report assists those individuals and groups in providing safer marine operating systems.

William H. Moore, Dr. Eng.

Professor Robert G. Bea

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

The sources of a majority (generally more than 80%) of high-consequence marine accidents can be attributed to compounded human and organizational errors (HOE) [Bea, 1989]. Recent examples include the *Exxon Valdez* tanker grounding (258,000 barrels of crude oil spilled), and the *Occidental Piper Alpha* North Sea platform explosions and fire (167 workers killed). At the initiation of this research in 1990, there was no structured quantitative approach to assist engineers, operators, and regulators of marine systems to either design HOE tolerant systems or to include considerations of HOE as an integral part of the design, construction, and operation of marine systems. The human element has generally been ignored.

The objective of this research is to develop engineering reliability and decision analysis procedures to assist in the assessment and implementation of alternatives for management of human and organizational errors (HOE) in operation of tankers and offshore platforms. The results from this research are intended to be used by engineers, operators, managers, and regulators concerned with preventing and mitigating the effects of HOE to increase safety of marine systems.

Five primary tasks were identified to reach this objective: (1) obtain well-documented case histories of tanker and offshore platform accidents whose causes are founded in HOE, (2) develop a classification framework for HOE, (3) analyze how HOE interactions caused the accidents, (4) investigate quantitative modeling methods to measure effectiveness and costs of alternatives that reduce the incidence and consequences of HOE, and (5) perform case history based evaluations of management alternatives.

Well-documented case histories of tanker and offshore platform accidents whose root causes are founded in HOE were identified, obtained, organized, and analyzed. An examination of current tanker and offshore operations was also performed. An organization and classification of the sources of HOE was developed. Analyses were performed to characterize how HOE interactions caused the accidents. A quantitative risk analysis (QRA) framework employing probabilistic, heuristic judgment, and influence diagrams were used to formulate these analyses.

Quantitative analyses of HOE-based marine casualties are studied using case histories and current operations as a framework for structuring influences, using influence diagrams, between critical events, decisions, actions, environmental inhibitors, and human errors. Quantitative measurement techniques were developed that incorporate the judgments and experiences of the users. Based on this framework, the effectiveness of various alternatives to reduce the incidence of HOE were investigated. Cost-benefit analyses were performed to illustrate evaluations of alternatives to identify the effective HOE reliability management measures.

1.1 BACKGROUND

Human errors have been shown to be the basic cause of failures of many engineered systems [Bea, 1989; Brown and Yin, 1988; Dougherty and Fragola, 1986; Heising and Grenzebach, 1989; Ingles, 1985; Moan, 1983; Nowak, 1986; Maritime Transportation

Research Board, 1976; Patè-Cornell and Bea, 1989; Royal Commission on *Ocean Ranger* Marine Disaster, 1985; Veritec, 1988; Wenk 1986]. Less than 20% of the causes of severe accidents involving these marine structures can be attributed to the environment. The rest of the causes are initiating events such as groundings, fire, explosions, and collisions. In almost all of these cases, the initiating event can be traced to a catastrophic compounding of human and organizational errors [Heising and Grenzebach, 1989; Offshore Certification Bureau, 1988; Maritime Transportation Research Board, 1976; Royal Commission on *Ocean Ranger* Marine Disaster, 1985].

The analysis of past decisions regarding the operations of tankers and offshore platforms provides numerous examples of instances in which organizational failures have resulted in failures of the marine systems [Heising and Grenzebach, 1989; Moan, 1983; Maritime Transportation Research Board, 1976; Patè-Cornell and Bea, 1989; Royal Commission on *Ocean Ranger* Marine Disaster, 1985; Veritec, 1988]. Either collections of individuals (organizations, societies) or single individuals (unilateral actions) contribute to accident situations. The errors range from those of judgment to "ignorance, folly, and mischief" [Wenk, 1986].

Traditional engineering of marine systems has focused primarily on the structure and equipment aspects, making sure that the right amount of structural materials is in place, that suitable functioning equipment is provided, and that the structure is constructable and serviceable for its intended purposes. Given that something in excess of 80% of failures of these systems have had causes founded in human errors, it is timely for engineers and regulators to begin to formally engineer human and organizational considerations into design, construction, and operation of structures. Those critical of the use of reliability based methods in engineering structures cite the omission of consideration of the "human aspects" as a primary obstacle to meaningful applications of reliability methods [Reid, 1989].

Studying the role of human errors in the reliability of engineered structures indicates that human errors and imperfections are basically inevitable [Bea, 1989; Dougherty and Fragola, 1986; Henley and Kumamoto, 1982; Ingles, 1985; Nowak, 1986]. These errors are influenced by cultural and moral values, corporate responsibilities and organizations, and individual training, craftsmanship, and integrity. The individual, organizations, and societies all play important roles in human errors.

Human errors originate from factors such as inattention or carelessness, inadequate training and testing (knowledge), wishful thinking, negligence, forgetfulness, and physical limitations (e.g. fatigue, seasickness). These errors are magnified and compounded in times of stress and panic [Heising and Grenzeback, 1989; Offshore Certification Bureau, 1988; Maritime Transportation Research Board, 1976; Royal Commission on *Ocean Ranger* Marine Disaster, 1985]. These errors can also be exacerbated by poorly engineered structures (that invite errors), and structures that are difficult to operate and maintain [Ingles, 1985; Melchers, 1987; Moan, 1983].

Operational failures can occur as a result of the willingness of an organization or individual to take a calculated risk [Arrow, 1951, 1972]. Failures can result from different types of errors that are bound to occur but can be corrected in time, provided that they are detected, recognized as errors and corrective action is promptly taken. Failures can also occur as the result of errors or bad decisions, most of which can be traced back to organizational malfunctions. For example, the goals set by the organization may lead rational individuals to make decisions and perform actions in a manner that corporate management would not approve if they were aware of their implications for reliability [Howard, 1966; Kahneman *et al.*, 1982]. Similarly, corporate management, under pressures to reduce

costs and maintain schedules, may not provide the necessary resources required to allow safe operations. The decision making ability of an organization affects its reliability and ability to operate safely.

Generally, two classes of problems face an organization in making collective decisions that result from sequences of individual decisions: information problems (who knows what and when?), and incentive problems (how are individuals rewarded, what decision criteria do they use, how do these criteria fit the overall objectives of the organization?) [Arrow, 1972; La Porte, 1988]. An emphasis of this research is on information (collection, communications, and learning), and on incentives, particularly as they affect the balancing of several objectives such as costs and safety under uncertainty in operating tankers and offshore platforms [Wenk, 1986; Weick, 1987].

The structure, the procedures, and the culture of an organization contribute to the safety of its product [Kahneman et al., 1982; La Porte, 1988] and to the economic efficiency of its risk management practices [Royal Norwegian Council for Scientific and Industrial Research, 1979; Wenk, 1986]. The organization's structure, for instance, can be hierarchical with little or no response to feedback from within the organization. As a result, safety problems may arise because of inconsistencies in the decision criteria (e.g. safety standards) used by different groups for different subsystems. Each level within the organization may have different views of organizational goals and methods of obtaining those goals. This partitioning may result in large uncertainties about the global system safety, about the reliability of the interfaces, and about the relative contribution of the different subsystems to the overall failure probability [Construction Industry Research and Information Association, 1977; Henley and Kumamoto, 1982; Moan, 1983].

The culture of the organization can also affect system reliability [Arrow, 1972; Wenk, 1986; Weick, 1987]. For example, the dominant culture may reward risk seeking (flirting with disaster) or superhuman endurance (leading to excessive fatigue), an attitude that in the long run may prove incompatible with the objectives of the organization. Another feature may be the denial of uncertainties leading to systematic biases towards optimism and wishful thinking [Maritime Transportation Research Board, 1976; Patè-Cornell and Seawell, 1988; National Bureau of Standards, 1985].

If organizational deficiencies affect a subsystem whose functioning is not highly critical, their effect on the reliability of the overall system is minor and may not justify profound organizational changes. However, complex interactions of relatively independently functioning subsystems have been found to substantially effect overall system reliability due to system complexities and tight coupling [Perrow, 1984]. If deficiencies affect a subsystem or a complex interaction of subsystems whose failure constitutes a system failure mode, it is urgent to address the problem at its human and organizational root. It is therefore desirable to link these failure contributors to the occurrence of the basic events of a probabilistic risk analysis [Dougherty and Fragola, 1986; Henley and Kumamoto, 1982; Moan, 1983] in order to gain a feeling for the urgency of remedial measures and to set priorities among HOE problems to be addressed.

In many cases, a combination of technical and organizational modifications can improve the overall safety level. In this research, the quantification of the benefits of HOE reliability management measures were developed using quantitative risk analysis (QRA) [Dougherty and Fragola, 1986; Heising and Grenzebach, 1989; Henley and Kumamoto, 1982; Moan, 1983; Nessim and Jordaan, 1985]. The analysis of a system's reliability allows identification of its failure modes and computation of their probabilities. It permits a decision maker to choose technical solutions that maximize an objective function (including reliability) under resource constraints [Wenk, 1986; Weick, 1987]. These so-

lutions include, for instance, the choice of operating procedures and equipment that minimize the probability of failure during the lifetime of a structure under constraints of costs, time to completion, production level, structure location and general type.

Technical modifications, however, represent only one class of risk management strategies. When a system's failure is studied after it occurs, it is often pointed out that what resulted in a technical failure was actually rooted in a functional failure of the organization [Arrow, 1972; March and Simon, 1958]. Organizational modifications may address some of the reliability questions at a more basic level than strengthening the engineering design alone. They include, for example, improving communications, setting effective warning systems, and ensuring consistency of standards across the organization.

1.2 METHODOLOGY

This research is an attempt, in the context of formal reliability analyses, is an effort to understand how human and organizational errors can influence the operation of tankers and offshore platforms; most importantly, to understand how checks and balances can be put in place to reduce the incidence of these errors, and to learn how to take advantage of "early warning signs" to interrupt catastrophic compounding of these errors [Construction Industry Research and Information Association, 1977; Dougherty and Fragola, 1986; Offshore Certification Bureau, 1988]. The approach used in this report is founded on five primary tasks discussed below. Figure 1.1 describes the inter-relation of tasks. These tasks are described in the scope of the *Management of Human Error in Operations of Marine Systems* project that formed the basis for this research.

Task 1. Identify, obtain, and analyze well-documented case histories of tanker and offshore platform accidents whose root causes are founded in human and organizational errors. Accident investigation reports by the U.S. Coast Guard, Minerals Management Service, and the National Transportation Safety Board, and information provided by U.S. ship and platform operators provide the majority of real-life case histories of operations-caused failures for this report. In addition, accident investigation reports by the Canadian Royal Commission (capsizing of the *Ocean Ranger*), the U.K. Department of Energy (*Piper Alpha* fires and explosions), and the Norwegian Petroleum Directorate (sinking of the *Alexander Keilland*) were obtained to provide additional case histories.

Task 2. Develop an organizational and classification framework for systematically identifying and characterizing HOE's. HOE classifications for the marine industry were reviewed and a practical error taxonomy was developed for the modeling framework to follow.

Task 3. Develop general analytical frameworks based on real-life case histories to characterize how human and organizational errors interacted to cause the accidents. Influence diagrams [Bea, 1989; Pate-Cornell and Bea, 1989] provide the basic analytical framework to develop simplified and generalized "templates" for tanker and offshore operations that preserve the central causative mechanisms, yet do not preserve the unique aspects of the particular disaster.

Task 4. Formulate quantitative analyses for the case histories based on *quantitative risk analysis* (QRA) procedures. These quantitative risk analysis procedures include the implementation of existing measuring techniques (probability encoding) and a probabilistic-heuristic approach of calculating a "safety index". The safety index (or conversely, the risk index) provides a relative measure of human errors influenced by events, decisions, actions, environmental conditions (inhibitors), system and task complexities, stress, and routine.

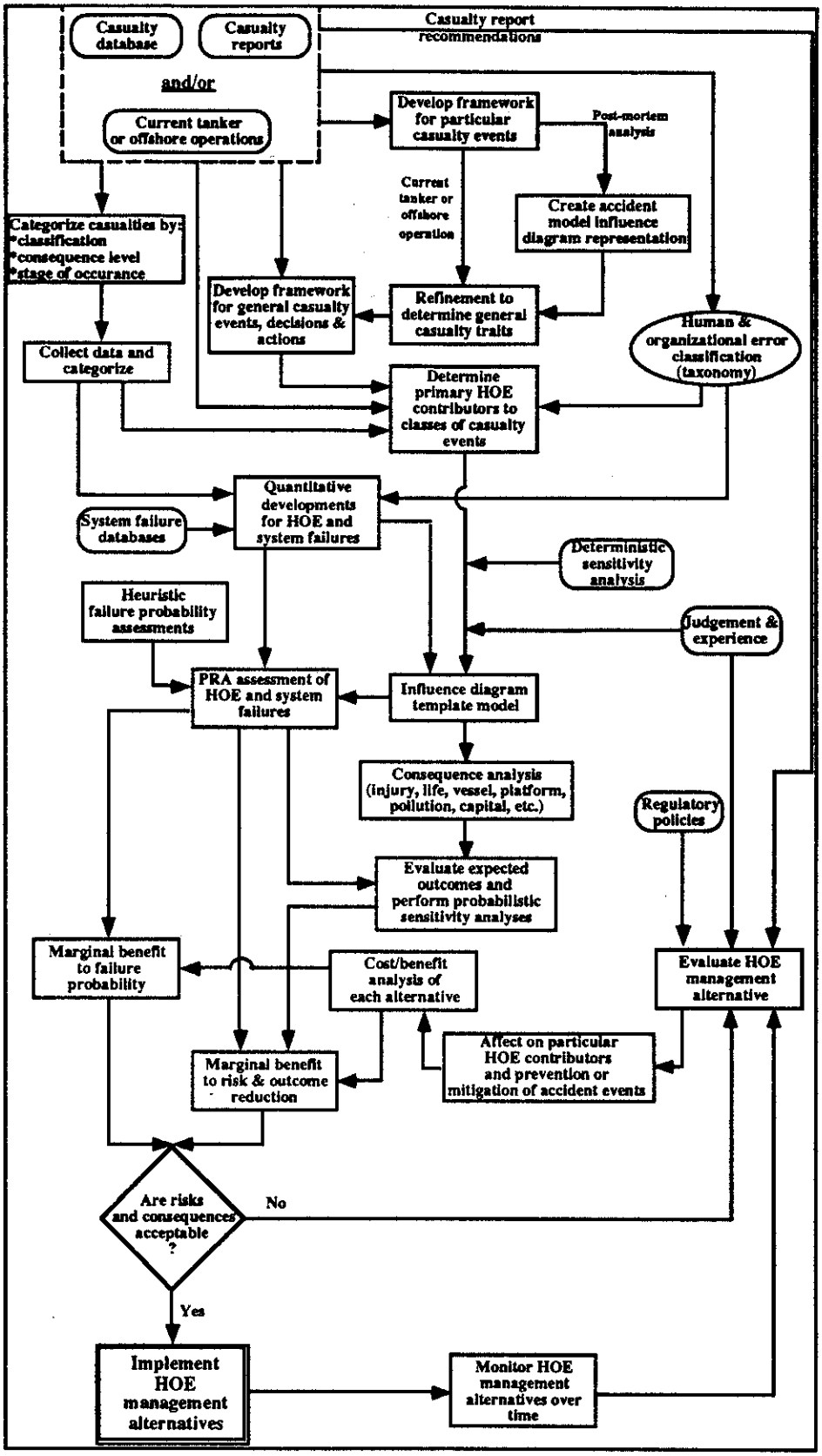


Figure 1.1 - HOE flowchart

These quantitative factors are then used as a basis from which to measure (using the influence diagram templates) the influences of human errors on the risks of accident scenarios.

Task 5. Investigate the effectiveness of various alternatives to reduce the incidence and effects of human and organizational errors. Alternatives are generated through regulatory, operator, and heuristic judgments. Evaluate the costs and benefits in terms of effectiveness of risk reductions (product of likelihoods and consequences). Case history-based evaluations and recommendations of the alternatives and tradeoffs are used to illustrate the processes associated with developing effective strategies for managing human and organizational errors in operations of tankers and offshore platforms.

The basic analytical framework is proposed using *quantitative risk analysis* (QRA). A QRA for engineering systems allows identification of the weakest parts of a system through qualification of the different failure modes [Henley and Kumamoto, 1982; Melchers, 1987]. This technique permits setting priorities among possible modifications aimed at the reduction of the failure risks resulting in optimal allocation of limited risk management resources.

A general method is to integrate elements of process analysis and organizational analysis in the assessment of the probability of system failure [Bea, 1989; Patè-Cornell and Seawell, 1988; Patè-Cornell and Bea, 1989]. Figure 1.2 provides a schematic description of the structure of this model. The first phase (which does not appear in this diagram) is a preliminary QRA to identify the key subsystems or elements of the system's reliability. The second phase is an analysis of the process to identify the potential problems for each of the subsystems and their probabilities or base rates per time unit or per operation.

Given that a basic error occurs, the next phase is an analysis of the human and organizational procedures and incentive system to determine their influence on the occurrence of basic errors and the probability that they are observed, recognized, communicated, and corrected in time (i.e., before they cause a system failure). The influence of human factors in QRA modeling is called *human reliability analysis* (HRA) [Bell and Swain, 1981; Swain and Guttmann, 1983].

The result of these three phases is a quantitative measurement of the possible types of structural defects and, therefore, to different levels of systems' capacity. The fourth phase involves a return to the QRA for the physical system and a computation of failure for each capacity level corresponding to the different system states.

A quantitative measurement of the overall failure is then obtained. It explicitly includes potential weaknesses in the different subsystems due to organizational factors. These different models (process, organization, and final QRA) have been integrated using an event tree [Dougherty and Fragola, 1986; Heising and Grenzeback, 1989; Nessim and Jordaan, 1985] or influence diagram [Shachter, 1986] to compute the failure probability under different circumstances (e.g., occurrence and correction of a given problem in the process).

In many cases, a combination of technical and organizational modifications can thus improve the overall safety level. It is proposed here to quantify the benefits of organizational measures using QRA as a starting point. This is the first attempt to structure a quantitative approach to assist engineers, operators and regulators to consider HOE as an integral part of design construction, and operations of marine systems. Given that this approach is in an early stage, focus is placed upon a broad number of aspects ranging

from individual human error to the organizational structure that may contribute to that error.

The main objective is to produce an applicable methodology and process to assess the impact of human error in operating marine systems. Further studies beyond the scope of this report can be conducted to focus on specific aspects to assess impacts of human factors and the details of the roles of organizational structures in operational reliability management.

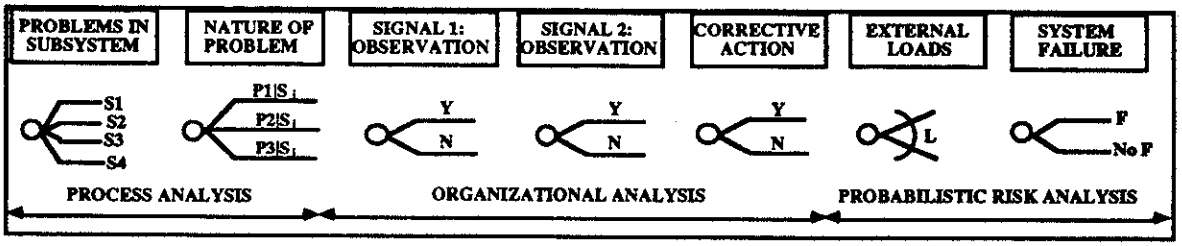


Figure 1.2 - Event tree showing the structure of the generalized reliability model [Paté-Cornell and Bea, 1989]

1.3 REPORT STRUCTURE

Chapter 1 provides the background and problem definition for the report. Five tasks describing the scope of the report. Five tasks describing the scope of the *Management of Human Error in Operations of Marine Systems* research project are defined. The methods to accomplish these tasks are also defined.

Chapter 2 reviews sources of well-documented case histories of tanker and offshore platform accidents whose root causes are founded in human and organizational errors. The two primary formats of casualty data were written accident reports and computerized casualty data. Casualty reports were collected from a variety of sources including the U.S. Coast Guard (USCG), National Transportation Safety Board (NTSB), Minerals Management Service(MMS), U.S. Geological Survey (USGS), U.K. Department of Energy and a number of additional sources. The chapter also discusses the state database information sources in providing safety information which have been collected. Casualty data collected by the USCG, Veritec, and the Institut du Français Petrole (IFP) provide the most current updated information on relating human errors to marine casualties and are described in Chapter 2.

Chapter 3 reviews existing marine casualty investigation reports, database, and error classifications to develop a practical human and organizational error classification framework. The HOE classification incorporates proposed taxonomies developed by the USCG and is supplemented by the addition of several key measures of human and organizational behavior and performance including violations, commitments to safety, and allocations of safety resources.

Chapter 4 discusses the development of general analytical frameworks based upon real-life case histories to characterize how the HOE's interact to cause accidents. The case histories, both post-mortem studies and currently existing operations form the basis from which accident characteristics are modeled. Influence diagrams are used to provide the basic analytical framework to produce simplified and generalized "templates" for tanker

and offshore operations that preserve the central causative mechanisms. The models are not created to predict a particular accident sequence, but to describe a general set of accident factors. For post-mortem studies, the models do not preserve the unique aspects of the particular disaster. Models of currently existing operations are developed from knowledge and experience to construct potential casualty scenarios. The influence diagram template provides a basis from which the user may view the dependencies of contributing factors to marine related casualties even though no quantitative assessments are made.

Once the templates are developed that relate relevant error contributors to the accident scenarios, the intent is to quantify the human errors conditional upon the error contributors. A quantitative measuring technique, the *Human Error Safety Index Method* (HESIM), has been developed in this research and is discussed in Chapter 5. The HESIM measures organizational, task and system complexities, and environmental factors that affect operators abilities to perform decisions, and actions to prevent or mitigate accident events. These measurement techniques rely upon judgments and experiences of those familiar with the operations being modeled and objective data to formulate a "safety index". A methodology for collection of the objective data, the *Human and Organizational Error Data Quantification System* (HOEDQS), has also been developed by this research.

The HOEDQS allows updating of human errors such that there becomes a greater reliance upon objective data and less reliance upon the judgmental indexing procedure. The strength of the data quantification system is that it is self correcting and has the capabilities of being updated and refined. The HESIM is used to assist in determining the impacts of organizational, system and task complexities, stress, routineness, and environmental conditions upon human errors and their effects upon increasing the risk. Error frequencies can be updated using the HESIM and HOEDQS and are then used to update the failure event index. The failure event risk index is then matched against the failure probabilities for that event. A functional relation between the risk index and probability of the accident event is then determined. This allows for forecasting of the risk of failure events for future operations under various human operator conditions to determine if these operational conditions lead to an acceptable level of risk.

Chapter 6 is an overview method from which to evaluate alternatives for HOE management and determine acceptable risks. Error frequency variations, influence diagram modeling variations, and cost-benefit analysis are described to evaluate HOE management alternatives. Two illustrations are provided: (1) tug escorts for tankers and gas leak detection, and (2) control for production platforms. Acceptable risks presented from both a historical and standards of practice viewpoints. An illustration of evaluating acceptable risks is also provided.

In Chapter 7, the methodologies discussed in Chapter 6 are applied to two well-documented case studies: the grounding of *Exxon Valdez* and the *Piper Alpha* disaster. The models developed in Chapter 4 are used as a framework to construct general models for two classes of marine casualties: (1) tanker grounding or collisions, and (2) platforms process leaks resulting from simultaneous production and maintenance. Influence diagram models are constructed from currently existing tanker and offshore operations: loading and discharge of tankers and crane operations for offshore platforms.

Chapter 8 discusses conclusions and recommendations. The conclusions discuss the strengths and limitations of qualitative and quantitative HOE analysis. The recommendations discuss directions for future HOE research in order to provide better quantitative analysis models of HOE in marine systems. The recommendations focus primarily on

measurements of contributing organizational errors, quantitative modeling, and HOE database developments.

Appendix 1 is a listing of literature related to human and organizational errors, influence diagrams, and human reliability and performance characteristics for both the marine and related industries. Influence diagram modeling, QRA modeling procedures and related information have been acquired and are presented.

Appendix 2 is a listing of all tanker and offshore platform casualty reports and database collected and discussed in Chapter 2.

Appendix 3 is the user manual for operating the HOEDQS and HESIM programs discussed in Chapter 5 and an operating guide for the influence diagram templates presented in Chapter 7.

Appendix 4 is a reference map of the steps used to perform an HOE analysis of particular classes of accidents. This is a consolidation of the methods discussed throughout the text into a short reference format.

Appendix 5 presents all other related publications by the authors of this report.

CHAPTER 2

CASUALTY DATA SEARCH

The first task of the HOE research project was to identify, obtain, and evaluate well-documented case histories of tanker and offshore platform accidents whose root causes were founded in human and organizational errors. The two primary formats of casualty data were written accident reports and computerized casualty data. A comprehensive listing of the accident casualty information and database are found in Appendix 1. The following summarizes the information collected to date:

1.) The U.S. Coast Guard (USCG) has supplied 18 written accident reports for tanker and mobile offshore drilling units (MODUs) casualties dated from 1979 to 1990. In addition, the marine casualty database (CASMAIN) which include 58,934 marine casualties dated through 1990 has been made available.

2.) The National Transportation Safety Board (NTSB) has supplied 47 written accident reports dating from 1980 to the present. The NTSB updates us with important accident reports as they become available.

3.) The Minerals Management Service (MMS) has supplied 20 written accident reports dating from 1979 to 1989 and offshore continental shelf accidents associated with oil and gas between 1956 and 1990. In addition, reports on risk analysis for offshore welding and crane accidents have been obtained.

4.) 10 independent casualty reports and inquiries have been obtained for catastrophic marine disasters such as *Piper Alpha, Ocean Ranger*, and the *Alexander Keilland.* These reports provide information on potential accident sequences, pre and post disaster design, operations, and regulations offshore.

5.) A number of marine casualty database information was collected and studied including the CASMAIN, World Offshore Accident Databank (WOAD), Institut Français du Pétrole (IFP), and the Marine Casualty Human Factors Supplement (MCHFS). The Offshore Reliability Data (OREDA) provides reliability information on safety, process, electrical, utility and crane systems, and drilling equipment. These database provide the most current updated information on relating human errors to marine casualties.

2.1 CURRENT MARINE SAFETY INFORMATION SYSTEMS

2.1.1 Written Accident Reports

Case histories are invaluable in that the study of a single case can provide insight into circumstances leading to catastrophic events. They allow one to examine causal factors which would be difficult to determine and identify by other means. Some catastrophic events are the result of a truly unique set of causal circumstances which allows one to examine the effects of contributing error factors and the limitations of human performance under various operating conditions [Reason, 1990].

However, case study analysis of marine casualties have numerous potential drawbacks. For instance, case studies are limited in the information available in that complex sets of events and circumstances leading to marine casualties tend to be "digitized". An overall picture of the complex processes and circumstances involved in the casualties is difficult to determine and present. Additionally, marine casualty investigators may be inexperienced and unaware of how to extract human factor data related causes to marine casualties. Another drawback is that there is no uniform description and recording system.

As a result, casualty investigators may report inaccurate information which is biased leading to difficulties in using the data for accident analysis.[1] Accident investigations and reports tend to focus on visibly "solvable" problems and thus are more interested in formulating "feasible" solutions and recommendations even at the expense of excluding valuable information. Solvable problems normally are not related to human error related factors and therefore are perceived as easier to fix. The majority of these solutions tend to be remedial in nature, non-effective, and can create unforseeable operational problems.

2.1.1.1 USCG and NTSB Reports

The written casualty reports provided by the USCG and NTSB have been valuable in examining a number of human and organizational factors involved in marine casualties. Though many of the reports tend to be technical in nature, most pay particular attention to the problems resulting from operator or management errors as well as point out the failure of operators to stay within the guidelines of marine regulations. The advantages of using USCG and NTSB for HOE study analyses are:

(1) Many of the accidents are of sufficient detail to formulate QRA to verify that the analyses can reproduce the results and implications of operations and general statistics of marine casualties.

(2) Each accident report is followed by recommendations which act as guidelines for operational procedure to minimize the chance of related accidents in the future. Alternatives for HOE management suggested in the recommendations can be analyzed to determine the effectiveness of these measures through the reduction of frequencies and magnitudes of these events (see Chapter 6).

2.1.1.2 Minerals Management Service Reports

Minerals Management Service offshore casualty reports are less detailed than those provided by the USCG and NTSB particularly in the technical areas. The reports make little mention of human factors contributing to casualties, however, a limited amount of human factor information can be drawn from the reports such as various concurrent activities which may have contributed to the hazardous environment (e.g. maintenance on risers resulting in loss of fuel containment and eventual ignition).

---

[1] Bias may be categorized in two ways by Spetzler and Staël von Holstein (1972):

(1) *cognitive* bias: "conscience or subconscience adjustments in a subject's responses systematically introduced by the way the subject is intellectually processing his perceptions... ", and

(2) *motivational* bias: "conscience or subconscience adjustments in a subject's responses motivated by his perceived system of personal rewards for various responses; he may want to influence the decision".

Two reports on OCS accidents do make mention of HOE related factors: *Risk Analysis of Welding Accidents: Gulf of Mexico OCS Region* (1967-1984) and *Risk Analysis of Crane Accidents* (1970-1984).

The *Risk Analysis of Welding Accidents: Gulf of Mexico OCS Region* report categorizes operator related events and errors by:

(1) lack of proper site preparation, coordination and supervision;

(2) failure to properly isolate potential source of fuel and/or flush /inert the work area,

(3) employee negligence,

(4) protective devices not used,

(5) poor housekeeping, and

(6) improperly prepared work area.

Ninety offshore welding accidents were recorded between 1967 and 1984 of which 88 accidents were the result of the causes listed above.

The report *Risk Analysis of Crane Accidents* categorizes 35 of 55 (64%) crane accidents as the result of:

(1) unsafe procedures (19 accidents),

(2) error of judgment (5 accidents), and

(3) crane overload (11 accidents).

No further differentiation of accidents stemming from human related causes were given.

An additional report, *Accidents Associated With Oil and Gas Operations: Outer Continental Shelf 1956 -1990* documented all OCS accidents during that time period. This report provides accident location, date, duration, type of accident, corrective action, volume of pollution spilled, fatalities, injuries, and damage to property or environment, but makes no mentions of the causes of casualty events.

In general, documentation of OCS casualties is limited and does not yield much detail to provide a solid basis to examine accident causes founded in HOE. Attempts to provide empirical risk analysis for offshore operations have been curtailed by lack of reliable data to examine human related factors [Laroque and Mudan, 1982; Carson, 1982]. In response to the *Piper Alpha* disaster, the Minerals Management Service (MMS) established a task group to examine the possibilities of similar disaster events and prevention and mitigation alternatives [Dandenberg and Schneider, 1991]. However, no mention was made of establishing effective measures to identify HOEs in the investigative process.

2.1.1.3 Independent Accident Reports

Independent reports on the *Piper Alpha*, *Ocean Ranger*, and *Alexander Keilland* disasters provide valuable information regarding HOE factors not normally seen with other accident reports. The Petrie and Cullen Reports provide valuable information on both technical and HOE related factors. The Petrie Report focuses primarily on technical

aspects of the disaster and makes available little information about HOE related factors though some mention of operational procedures is included. The Lord Cullen Report is a detailed study examining technical, and human and organizational errors in both design and operations. In addition, the report provides recommendations for future platform operations along the United Kingdom OCS. The Report of the Royal Commission on the *Ocean Ranger* disaster (1985) provides valuable information on technical, human, and organizational factors which supplement the USCG technical related report. Reports on the *Alexander Keilland* are also available but direct attention is given primarily to technical issues.

2.1.2 Accident Data Bases

2.1.2.1 CASMAIN marine casualty database

The USCG vessel and personnel casualty database (CASMAIN) is currently the United States Coast Guard Marine Safety Evaluation Branch's primary source of vessel and personnel casualty data. Though CASMAIN is primarily single dimensional, task oriented, and lacks documentation of complex interaction of human errors, it established a basic taxonomy of human and organizational factors [Dynamic Research Corporation, 1989] and is listed in Table 2.1. Table 2.2 provides the human and organizational error classification used in the CASMAIN.

CASMAIN was developed by the USCG to document both vessel and personnel casualties. The primary sources of information are the "nature" (event) and "cause" (reason) for the casualties. Both the nature and cause categories have designations for human errors in their taxonomies. The nature category includes collisions, disappearances, explosions, fires, groundings, and material failure. The cause category provides the reasons for each nature described in the database.

The general structure of CASMAIN has a maximum of three fields for the "nature" and a maximum of seven fields for "cause" (see Figure 2.1). Each of the nature fields are labeled Nature 1-3 in the progression of failure events. The nature of the incident follows through various stages of events leading to a final outcome. Generally each accident has a set of causes associated with that event as observed. For example, Figure 2.1 demonstrates the three nature fields in CASMAIN representing the *Ocean Ranger* accident (84 men killed off Newfoundland; February, 1982).

The CASMAIN database has the advantage of providing a basis for establishing empirical models for statistical models for various HOE forms. However, there are limitations to its use in analyzing contributing HOE factors. First, error sequences are "digitized" from what initially were a set of complex and continuous events into a limited number of events and circumstances. Many of the error sequences and interactions cannot be analyzed through CASMAIN since information is often incomplete or inaccurate. Second, there is no way to trace individual errors grounded in organizational structure since the database is limited in organizational error identification. Third, CASMAIN is primarily task oriented and does not correlate associating events and errors at different states or stages of the system failure. Finally, there is no methodology for differentiating among various organizational parties at fault in the accident sequence in order to determine causation.

Returning to the example of the *Ocean Ranger*, there were a particular number of causes for the three "natures" (events) described. In examining the written accident reports for the disaster, it is evident that there were substantially more causes related to the events of the accident than those described in CASMAIN [Royal Commission on *Ocean Ranger*, 1985]. In addition, a number of factors were involved regarding the regulatory require-

ments for manning the *Ocean Ranger*. The government of Newfoundland was persistent in having the platform manned with Canadians even though they were not properly trained [Royal Commission on *Ocean Ranger*, 1985].

Table 2.1 - CASMAIN nature categories

Allision	**Collision**	**Material failure**
	meeting	main engine/motor
Barge Breakaway	crossing	boiler
	overtaking	main steam system
Capsizing	special circumstances	auxiliary steam system
	w/ ice	feed - condensation system
Disappearance	w/ aid to navigation	cooling water system
w/ trace	submerged object	fuel oil supply
w/o trace	floating object	lube oil supply
	bridge	main generator
Fire	pier/dock	auxiliary generator
vessel furnishing	offshore drilling unit	electrical control system
vessel cargo, freight	fixed object NOC	electrical display system
machinery space	NEC	hydraulic control system
pumproom	unknown	pneumatic control system
vessel structure	w/dike, lock, or dam	bilge system
vessel fuel		reduction gear
electrical	**Explosion**	shaft system
vessel cargo, fuel	machine space - no fire	propeller
vessel cargo, HAZMAT	pressure vsl - no fire	cargo handling-tanker
NEC	pumproom - no fire	cargo handling-freight
	boiler - no fire	salt water system
Foundering	fuel - no fire	venting system
sinking	cargo - fire	inert gas system
w/o sinking	machine space - fire	crude oil washing system
	pressure vsl - fire	navigation equipment
Grounding	pumproom - fire	ground tackle
accidental	boiler - fire	lifesaving equipment
intl w/ damage-hazard	fuel - fire	fire fighting equipment
	NEC	personnel protect equipt
Steering System Failure	unknown	hull-structural
control system		hull-deterioration
rudder and shaft	**Cargo loss or damage**	
		Swamping
Disabled	**Swamping**	
		Well Blowout
Wake Damage	**Weather Damage**	

Table 2.2 - CASMAIN human error classification

-Bypass available safety devices	-Inattention to duty
-Intoxication (alcohol-drugs)	-Calculated risk
-Carelessness	-Error in judgment
-Lack of knowledge	-Lack of training
-Lack of experience	-Operator error
-Fatigue	-Smoking
-Open flame	-Stress
-Physical impairment	-Psychological impairment
-Failed to comply with rules, regulations or procedures	-Inadequate supervision
-Improper casualty control program	-Improper safety precautions
-Failed to account for current-weather	-Failed to account for tide
-Failed to use available navigation equipment	-Failure to ascertain position
-Failed to use charts and publications	-Failed to use radio-telephone
-Relied of floating aid to navigation	-Failed to yield right of way
-Failed to establish passing agreement	-Failed to keep to right of channel
-Failed to proceed at safe speed	-Failed to stop
-Failed to keep proper lookout	-Improper-faulty lights-shapes
-Improper-missing whistle signal	-Improper maintenance
-Used defective equipment	-Design criteria exceeded
-Service condition exceeded	-Improper loading
-Preventative maintenance not done	-Improper cargo storage
-Improper securing-rigging	-Improper mooring-towing
-Inadequate fire fighting equipment	-Inadequate lifesaving equipment
-Inadequate controls	-Inadequate displays
-Inadequate statutory-regulation requirements	-Inadequate owner-operator
-Inadequate owner-operator safety program	-Inadequate manning

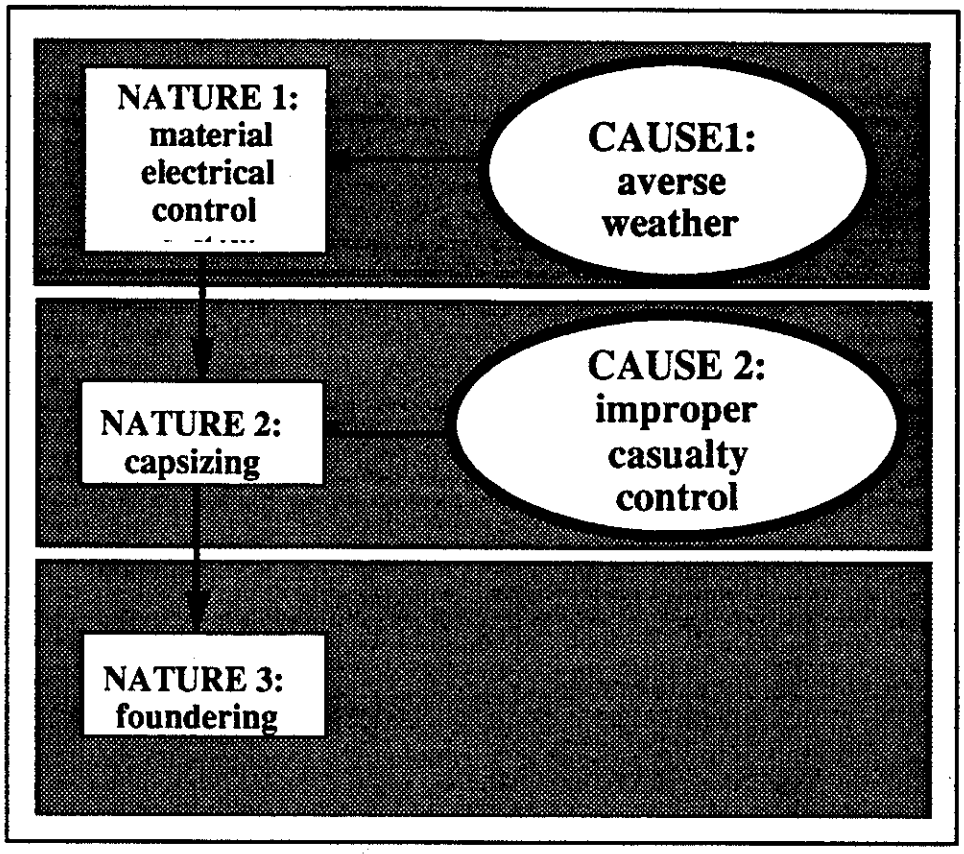


Figure 2.1 - CASMAIN database accident nature and cause relationship for the *Ocean Ranger* disaster

Using the CASMAIN error classification, Figure 2.2 demonstrates a more detailed version of the cause-event interaction. Even in documenting the causes to each nature, there is a loss of complex and dynamic interaction. It is difficult to determine whether human errors are the result of errors rooted in organizations or whether they are the result of individuals acting on their own initiative.

It is virtually impossible to distinguish between responsible parties of various errors in the sequence particularly for offshore operations where many sub-contractors may work aboard the vessels. For example aboard the *Ocean Ranger*, Mobil Oil was the operator, while the ODECO Drilling Company was the contracting company operating the semi-submersible drilling unit. Though both organizations were at fault, the error classification did not differentiate the degree of fault or circumstances of fault between contributing management parties.

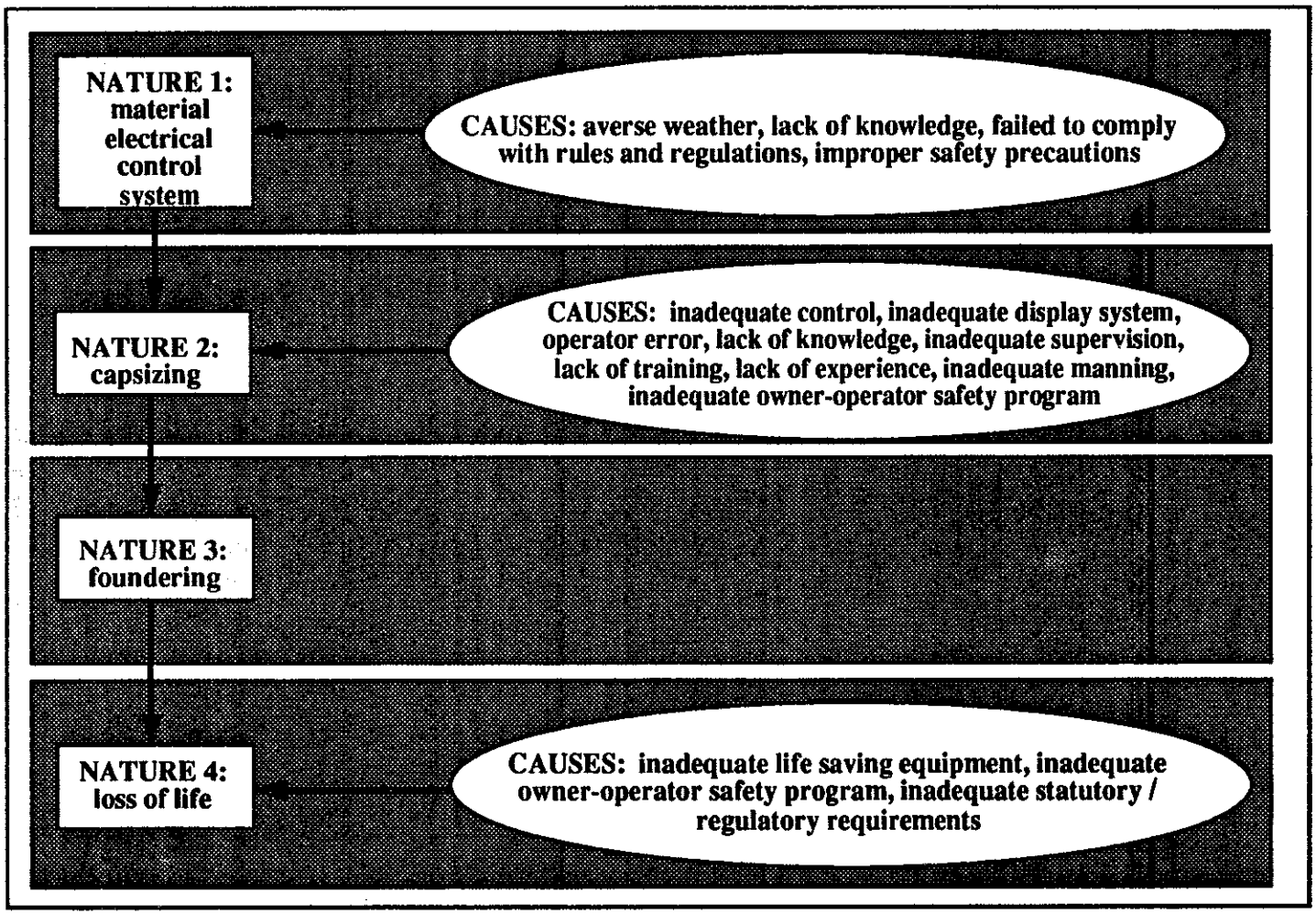


Figure 2.2: More detailed CASMAIN database accident nature and cause relation for the *Ocean Ranger* accident

2.1.2.2 Marine Casualty Human Factors Supplement

The *Marine Casualty Human Factors Supplement* (MCHF) is a recent development from the USCG to supplement the CASMAIN database as a tool for documenting capturing the human element in marine casualties [USCG, 1992]. The MCHF relates casualty related error information to the role, position, and education of the personnel involved in the marine casualty.

However, there is little or no indication that the MCHF captures the complex interactions leading to accidents in a dynamic fashion as initially described for the *Annotated Human Factors Taxonomy* (AHFT) developed by Dynamic Research Corporation (1989). The AHFT provided a comprehensive, in-depth description of how to identify the complex interactions related to marine casualties (see Chapter 3 for background on HOE classification). The Marine Casualty Human Factors Supplement (MCHF) was modified by the USCG as an alternative to the AHFT and has been designed to work within the CASMAIN format described above.

As shown in Table 2.3, MCHF categorizes HOE factors into classes and related subclasses. Then as shown in Table 2.4, the state of the human error class or subclass is also associated with the particular error contributing factor. For example, a *communication* error (class) due to *phraseology* (subclass) was *misunderstood* (state) leading to an improper action or decision. Though the MCHF is used to provide further details for documentation of human error contributors, it does not allow for documentation of errors at different stages within the accident scenario and therefore suffers from the same single dimension modeling problem as with the CASMAIN.

2.3.3 World Offshore Accident Database

The World Offshore Accident Database (WOAD) is the world's largest offshore casualty database. The advantage of using WOAD is that it provides global statistics on offshore casualties. WOAD allows comparison of offshore operations worldwide, and is conducted in U.S. Offshore Continental Shelf (OCS) waters and allows for the analysis of time dependent trends in offshore safety for various types of operations (drilling, production, fixed platforms, mobile offshore drilling units (MODUs), etc.).

Veritec, by its own admission directly acknowledges the need for modifying WOAD to account for worldwide operational safety and human factors. The database is limited to documenting events which have initiated the accident chain with little or no mention of the causes of accident events [Bekkevold, *et al.*, 1990; Veritec, 1988]. WOAD uses the following fields of human related errors:

-Unknown	*-Unsafe act*	*-Improper design*
-Improper equipment used	*-Sabotage*	*-Open flame*
-Unsafe procedure	*-Safety system malfunction*	*-Smoke-match ignition*
-Collision w/ vessel passing by	*-Welding-cutting torch ignition*	*-Other*

The database is similar in nature to CASMAIN and provides little information on the detailed chain of nature-cause relations between accidents.

2.3.4 Institut Français du Pétrole (IFP)

The Institut Français du Pétrole (IFP) is a database consisting of both tanker and offshore related casualties worldwide since 1955. This database is divided into two categories: (1) tanker accidents resulting in spills of at least 500 metric tons, and (2) platform accidents resulting in the shutdown of activity for a minimum of 24 hours for both drilling and production platforms.

Table 2.3 - MCHF supplement human factor classification and sub-classifications

Communication -clarity -language -phraseology **Knowledge-proficiency (training and experience)** -damage control -draft-air draft -emergency procedure -general knowledge -job-task response -maneuvering -route-environment -rules, regs, policy -stability-trim -system-equipment operation -vessel operation **Management** -discipline -job description -personnel coordination -personnel qualification -personnel sufficiency -personnel-task matching -personnel training policy -supervision -task loading -tests-drills **Equipment status signals and indicators** -accuracy -clarity -consistency -credibility -discrimination -resolution	**Mental influences** -anxiety -apprehension -boredom -complacency -deliberate misaction -distraction -equipment confidence -expectancy -habit interference -inattention -interpersonal relationships -mental capacity -management induced pressures -motivation -panic -perception -self confidence -self discipline -self induced pressures **Physical influences** -alcohol -chronic fatigue -drugs -hearing problem -medication -illness -short-term fatigue -toxic substance -visual problem **Compliance with rules, regulations, policy** -availability -clarity -currency -sufficiency

Table 2.4 - MCHF supplement human factor states

-attempted	-inadequate	-not performed
-bypassed	-incorrect	-not possible
-continued	-ineffective	-not present
-delayed	-initiated	-not reached
-disregarded	-misinterpreted	-not received
-exceeded	-misjudged	-not secured
-excessive	-misunderstood	-not sought
-ignored	-not attempted	-not used
-improper inspection	-not clarified	-overestimated
-improper maintenance	-not determined	-performed
-improper use	-not followed	-reached
-improper	-not known	-underestimated
-imprudent	-not monitored	

These databases exclude some accidents that may have resulted in injury or loss of life because they did not result in oil discharge or work stoppage. One particular advantage of the IFP is that it has two types of data input fields: (1) digitized fields with well defined inputs and abbreviations, and (2) informational inputs. The digitized fields that are similar to the CASMAIN, WOAD, and the MCHF are used for statistical uses in analyzing accidents. On the other hand, the informational inputs are for documenting information that is not easily captured in the digitized fields. For example, in one incident, 10 crewmen abandoned ship and were killed by sea snakes [Bertrand and Escoffier]. This type of information is not easily captured in a standardized digital database but can be captured in the informational inputs.

Similar to the WOAD, the IFP database allows for global analysis of both tanker and offshore casualties but fails to capture relevant information related to HOEs. In addition, the IFP does not document near miss data, minor casualties, or malevolent behavior (e.g. scuttling of ship by the crew). These factors limit IFP's use in studying the complex interactions between HOEs and marine casualties.

2.2 EXISTING MARINE RELATED ERROR CLASSIFICATIONS

2.2.1 Marine Board Error Classification for Marine Casualties

The Maritime Transportation Research Board (MTRB) conducted a five year study on merchant marine safety entitled *Human Error in Merchant Marine Safety* (1976). The objective of the study was to determine the causes of marine casualties resulting from human errors. The MTRB panel concluded that there were 14 human factors which led to marine casualties or near casualties. These factors include a mixture of both causes and effects. For example, *inattention* (effect) can be the result of *inefficient bridge design* (cause) or an ambiguous *pilot-master relationship* (effect) can possibly be the result of *inadequacies of the rules of the road* (cause).

(1) *Inattention*: lack of full vigilance to duties and responsibilities assigned.

(2) *Ambiguous pilot-master relationship*: confusion in authority and responsibility.

(3) *Inefficient bridge design*: poor instrumentation and control stations.

(4) *Poor operational procedures*: failure of deck and engine watchstands to observe consistent operating standards.

(5) *Poor physical fitness.*

(6) *Poor eyesight.*

(7) *Excessive fatigue.*

(8) *Excessive alcohol use.*

(9) *Excessive personnel turnover.*

(10) *High level of calculated risk.*

(11) *Inadequate lights and markers: particularly for vessel navigation purposes.*

(12) *Misuse of radar*. Misuse or misinterpretation of radar equipment.

(13) *Uncertain use of sound signals*: general failure to employ sound signals as required for rules of the road.

(14) *Inadequacies of the rules of the road*: when rules are considered to be the source of, rather than the countermeasures to human error casualties.

These conclusions were based upon an intensive literature search as well as 359 in depth interviews conducted with pilots, masters, deck officers, chief engineers, engineering officers, tug and harbor personnel.

In addition to these human factors, the panel concluded there is an inadequate database to maintain statistics on marine casualties and recommended the development of such a database by the USCG. The MTRB panel also made recommendations to address the 14 human factors listed above.

Additionally through examination of the questionnaires and literature search, the MTRB panel defined 13 types of human errors they believed to be detrimental to safe marine operations:

**Panic or shock*
**Drunkenness or drug influence*
**Inattention*
**Anxiety*
**Negative transfer of training*
**Ignorance*
**Fear*
**Sickness*
**Confusion*
**Incompetence*
**Fatigue or drowsiness*
**Negligence*
**Calculated risk*

2.2.2 Errors Induced by Organizations in Platform Casualty Analysis

Patè-Cornell and Bea (1989) suggest an organizational error taxonomy for design, construction, and operations of offshore platforms defining organizational errors as: (1) individual errors "grounded" in the organizational structure, and (2) legitimate and rational decisions by the individual which are in variance with the standards of the organization. This classification of operator errors can be used to relate individual errors with those rooted in the organizational structure. Previous analysis of organizational

errors in design, construction and operations of platforms have resulted in quantitative assessments of alternatives to improve reliability through organizational modifications.

Organizational errors can be the result of three major sources: (1) human limitations (e.g. fatigue, seasickness, etc.), (2) lack of communication and transfer of relevant information to decision makers at appropriate management levels, and (3) incentive problems resulting from incompatibility of goals and preferences between various levels of management and specific actors.

Figure 2.3 shows the classification developed to address organizational errors. The taxonomy distinguishes *gross errors* and *errors in judgment*. Gross errors are those resulting from a lack of knowledge, understanding, and the inability to respond under various circumstances. Gross errors are also errors in which there is little controversy or ambiguity and the individual would take notice of the error if brought to his attention. Errors in judgment are interpretations of available information which may be incomplete or uncertain and the resulting decisions are often ambiguous.

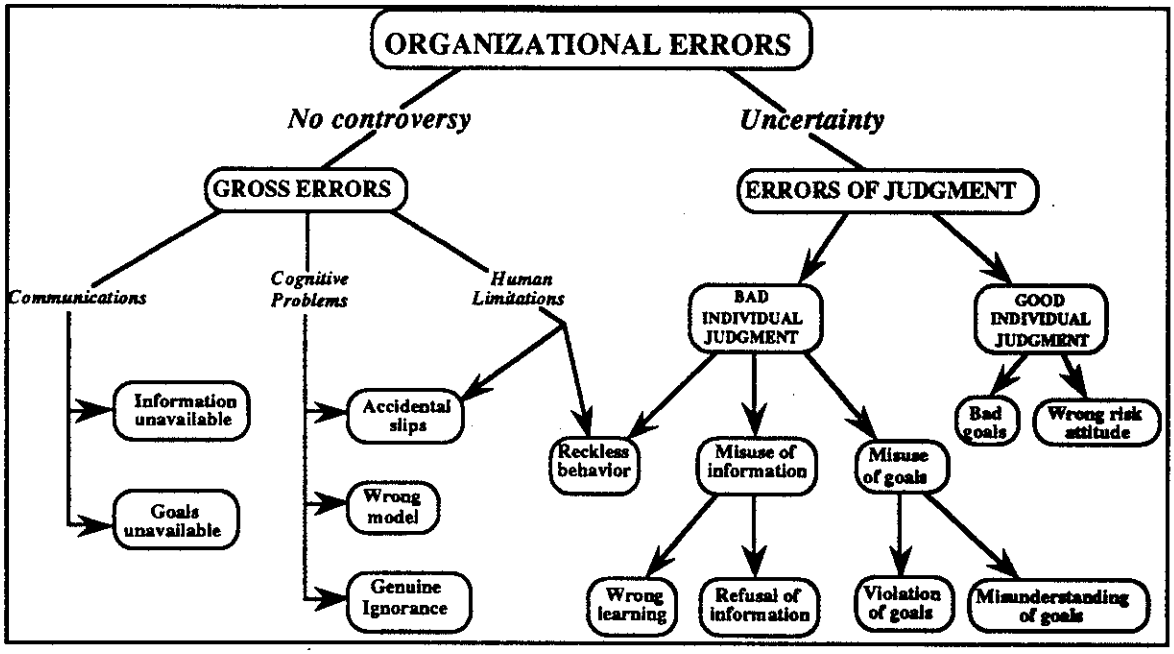


Figure 2.3 - A taxonomy of organizational errors [Paté-Cornell and Bea, 1989]

Gross errors can be further differentiated into communication and cognitive problems, and human limitations. Communication errors are those where information is not available to the decision makers at specific levels because the information may not have been gathered or the proper communication channels do not exist between involved parties. In addition, the goals may not be communicated sufficiently to illicit proper actions.

Cognitive problems are divided into accidental slips, incorrect perception (wrong model), and genuine ignorance. Accidental slips are those errors resulting from such aspects as work overload, stress, and improper job design. An individual in the organization may firmly believe in a wrong model because of errors in interpreting incomplete information. In the third case, the individual may be unable or unwilling to acquire additional

information and thus is genuinely ignorant to the situation. Human limitations can result from either physical or psychological factors due to inadequate hiring practices or bad individual job design.

Errors of judgment are differentiated into bad and good individual judgment. Bad individual judgment can be in operational behavior, misuse of information, or goals of the organization. Errors of judgment may also occur when inadequate procedures and organizational structures lead to rational decisions at odds with the overall objectives of the organization.

2.3 SUMMARY

The current state of written casualty reports and databases leads to the conclusion that little good information is available to study the complex interactions of human errors in operations of marine systems. This problem is not unique to the marine industry (Swain and Guttmann, 1985). The most reliable sources incorporating HOE related factors tend to be the written reports. Yet, as concluded by Marton and Purtell (1990), there currently exists:

(1) no comprehensive, standardized, validated and commonly accepted classification of human factors to adequately identify human factors involved in the casualty process;

(2) no standardized, hierarchically organized, concept or format for identifying human factor casualty data to identify and correlate direct error causes to the underlying and contributing factors that shape the behaviors responsible for error and accident events; and,

(3) no commonly accepted data collection concepts or methodologies that assist marine casualty investigators to accurately detect, describe, and record the key human error elements correlated with marine casualties.

CHAPTER 3

HUMAN AND ORGANIZATIONAL ERROR CLASSIFICATION

The purpose of Task 2 was to develop an organizational and classification framework for systematically identifying and characterizing various types of human and organizational errors.

This chapter develops a practical human and organizational error classification framework that uses existing marine casualty investigation reports, databases, and error classifications. The HOE classification incorporates proposed taxonomies developed by the USCG and is supplemented by the addition of several key standards by which measures of human and organizational behavior and performance including violations, commitments to safety, and allocations of safety resources are identified.

3.1 BACKGROUND -CHARACTERIZING ERROR AND FAILURE FACTORS

As stated by Reason (1992), effective safety management can only be obtained by having relevant up-to-date information on the reliability of the operating system. System reliability is continually in a state of flux as a result of changes in economic conditions, management, organizational culture, variability in human performance, changes in technologies, degradation of operating systems, and variability in environmental conditions. To gauge a system's reliability, it is imperative to maintain a relevant up-to-date information system that properly identifies casualty contributing factors. Like most industries with low probability high consequence accidents (e.g. nuclear power, air traffic control, aircraft carrier flight operations, etc.), the tanker and offshore industries operate with the reliability of the safety factors varying in time. As shown in Figure 3.1, these *intrinsic safety factors* are dependent upon measures of human, organization, and system performance.

Safety factors can be gauged for activities as they interact to affect the system. For example, the "design" of the system may be at either extreme. For instance it may be too complex and weakly linked or simple and robust. However, most operational systems lie between the two extremes. Perrow (1984) discusses that complex systems may be tightly coupled and too difficult to operate safely (destined to failure) even though it is robust. On the other hand, a simple system may be weak linked (tightly coupled). Each of the factors are assessed through the *safety information system* which determines the "temperature" (reliability) of the system. The basis of safety information systems lies in the development of a taxonomy to identify human factors contributing to a potential accident scenario. Figure 3.2 demonstrates five elements which relate to accident causation [Reason, 1992].

Defenses are placed in the system to reduce the chances of accidents or incidents based upon contributory human factors. The defenses may be systems (e.g. redundancy, high load capacity) or operations (e.g. safety programs, regulations).

Reason (1992) classifies human failures into *types* and *tokens*. Failure types are those which are founded in organizational, management, and regulatory culture, policies and pro-

cedures. The failure types can be further distinguished into *source* and *functional* types. Source type failures are decisions made at the strategic level of the organization. Functional types failures are made at the line management level where strategic errors manifest into functional form. Tokens are subdivided into *condition* and *unsafe acts*. Condition tokens are dependent upon psychological or conditional states of the operators or system which lead to unsafe acts at the operator crew level. Unsafe act tokens are categorized as "slips", "lapses", "mistakes", or "violations".

In examining the effects of human errors in marine systems the most available and widely used sources of safety information are casualty and incident reports. However, casualty and incident reports do not always capture important underlying causes of accidents and incidents [Moore, 1991; Marton and Purtell, 1990; Laroque and Mudan, 1982; Panel on Human Error in Merchant Marine Safety, 1976]. Casualty reports were used to examine human, organizational and system errors leading to catastrophic consequences in tanker and offshore platform operations with relative success in identifying the relevant HOE factors [Paté-Cornell, 1992; Roberts and Moore, 1992].

However, current changes in operational procedures resulting from accident analyses tend to lead to ad hoc human and organizational error management alternatives. For example, the *Oil Pollution Act of 1990* (OPA 90) requires all new tankers to be constructed with double-hulls to reduce the likelihood of hydrocarbon spills in the event of collision or grounding. The decrease in vessel capacities (as much as 40%) results in the necessity for more vessels to keep pace with the volume of demand. This can lead to higher vessel traffic and possibly increase probability of vessel collisions [Bea and Moore, 1993].

A logical progression in gathering system safety information is to examine unsafe act errors and violations which directly lead to accidents and incidents. Unlike the commercial aviation industry, there is no established reporting system in the marine industry to gather information on unsafe act errors and violations. The commercial aviation industry maintains the *Aviation Safety Reporting System* (ASRS) which receives, processes, and analyzes voluntarily submitted aviation incident reports by pilots, air traffic controllers and other industry sources. Efforts to develop a similar system for the marine industry have been in vain.

Unsafe acts in the marine industry have generally been kept in confidence by the operators. Unsafe acts are violations and the result of motivation, individual and management attitudes and cultures which are founded at higher levels in the organization. For example, at the time of the *Piper Alpha* disaster, simultaneous maintenance and production were being performed on the platform which led to a succession of explosions and fires killing 167 men and destroying the platform. The problem was founded not only at the front-line operator level, but in the organization which allowed the simultaneous operation to maintain production schedules [Paté-Cornell, 1992].

The next level in the safety information system scheme is the condition tokens. Condition tokens are psychological and situational precursors to accident scenarios. They are factors which contribute to unsafe acts such as hazardous working environments, job design, and inadequate training. Each of these condition tokens' root causes are found in critical underlying contributing errors. For example, the day before the *Piper Alpha* disaster, the Offshore Installation Manager (OIM) left the platform and temporarily promoted other people to compensate for his loss rather than bringing aboard a qualified OIM. The acting OIM was unable to coordinate an evacuation during the crisis eventually leading to his death and that of 83 other men in the accommodations unit [United Kingdom Department of Energy, 1990]. The acting OIM was inadequately trained for the job even though the underlying contributing causes were founded at the management level since qualified person

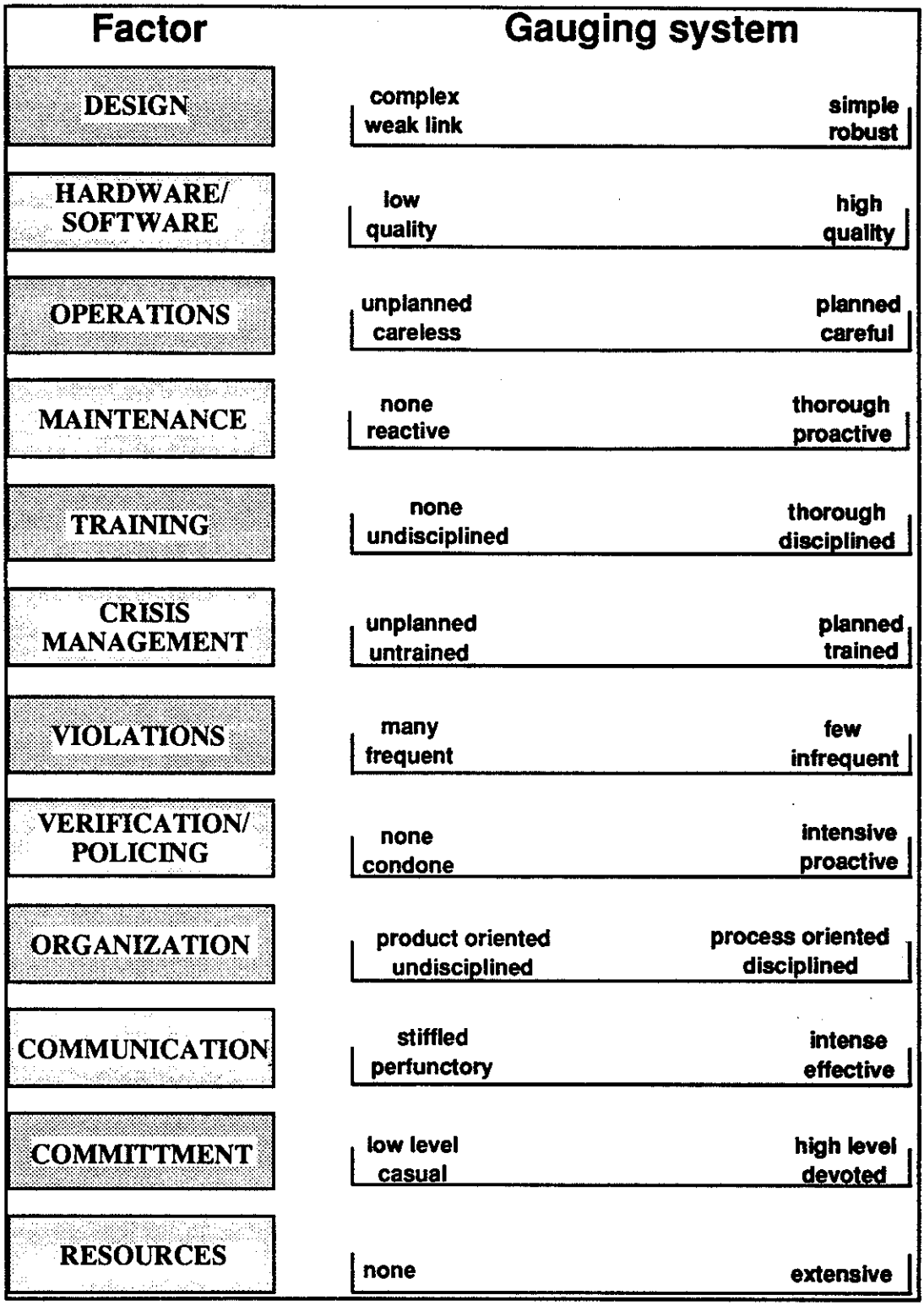


Figure 3.1 - Operating system profile

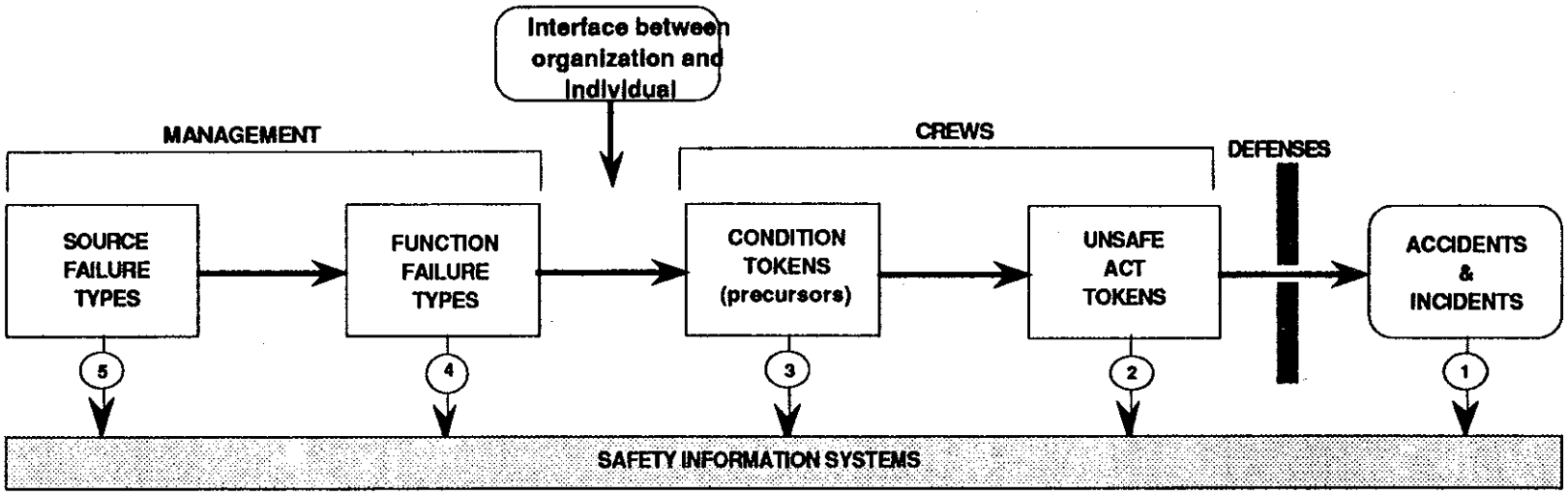


Figure 3.2: The basic elements of safety information system as they relate to the type-to-token stages involved in accident causation. [Reason, 1992]

nel were not present during critical operations. This is an example of a situational condition that compounded the catastrophic loss of life and platform.

Assessing safety information of functional failure types begins by addressing the "intrinsic safety health of an organization" [Reason, 1992]. For example, general failure types can be categorized as: inadequacies in operating procedures and conditions, system defects and inadequate defenses, communication failures, poor maintenance, design failures, and so on.

Finally, addressing source failure types looks towards long-term safety goals of the organization. This can be directed at top-level management's commitments to safety, competence in addressing problems, or a lack of cognizance of the problem's nature. Though there is no standardized form to assess these issues, Reason (1992) categorizes the states of organizational behavior toward safety practices as:

(1) *Pathological*: Safety systems are at minimum industry standards, no top-level management commitments toward safety goals. Hungarian nuclear power industry, Bhopal Union Carbide chemical plant prior to accident in 1984.

(2) *Incipient reactivity*: Staying just one step ahead of regulations and showing signs of concern for accident trends. Occidental Petroleum - Aberdeen prior to *Piper Alpha* disaster.

(3) *Worried-reactive*: Concern about continual trends in close calls, incidents and accidents in its operations. Offshore production platforms with histories of close calls leading to shutdown of production.

(4) *Repair-routine*: Reasonable sensitivity to past and potential future accident events, safety data collected (accidents and incidents) and remedial safety measures implemented on a local level. Well operated offshore platforms ten years ago.

(5) *Conservative-calculative*: Conduct a range of auditing techniques and workplace safety measures. Concerned with "techno-fixing" safety measures for humans and operating systems (i.e. better hardware and ergonomics). U.S. nuclear power industry (currently moving toward *incipient proactivity*) and well operated offshore platforms and tankers prior to *Piper Alpha* and *Exxon Valdez*.

(6) *Incipient proactivity*: Moving away from engineering fixes and acknowledge the role of organizational culture, policy, and procedures in the reliability of the operating system and actively searching for better human error management alternatives. U.S. nuclear power industry (in near future).

(7) *Generative-proactive*: Large number of proactive measures in place, top level commitments to safety, safety measures continually being assessed and updated, and a lack of complacency among management. Flight operations for aircraft carriers and the Federal Aviation Administration.

3.1.1 Issues in Establishing an HOE Classification

One of the keys to developing an effective classification is to determine the goals and preferences of the model user. For example, tanker or offshore platform operators may wish to establish error classifications and models which focus on specific areas of operation for allocation of limited resources. These goals and preferences may be established in the classification to examine the effects of the operating alternatives weighing

safety, economic, and production costs and benefits as the driving force. On the other hand, regulators and policy makers may wish to establish environmental, economic and social risks and costs of specific tanker and offshore operations. In short, the taxonomies and models would vary to project the preferences of the user in examining costs and benefits of these operations.

The complexity of the classification must be weighed against the time, available resources, goals and preferences of the user. A primary problem in classifying errors is striking a balance between a general error taxonomy addressing general adaptive processes or basic error tendencies, and highly detailed examinations of specific error forms [Reason, 1990]. Users must ask themselves if the marginal value of information gained, as the model constructed becomes more complex is worth the additional input of resources. For example, the user may wish to establish a general framework model with only limited detail and spend more time on analysis and examining the effects of sensitivity and uncertainty in the model. Yet another individual or group may wish to develop a meticulously detailed error classification and model formulation at a substantial cost in time and resources. This preference allows the user to examine finely detailed aspects of human performance or limit the amount of ambiguity and uncertainty in the classification and model formulation.

The goal of establishing this classification is to develop an organizational classification framework for systematically identifying and characterizing various types of marine related human and organizational errors. The classification should be commonly agreed upon and practical for engineers, regulators and decision makers. In addition, the classification should be simple enough for a range of experience and expertise levels to use, yet robust and detailed to allow users to adequately model the marine operating system.

3.2 HUMAN and ORGANIZATIONAL ERROR CLASSIFICATION

The problems stated above led the U.S. Coast Guard (USCG) to develop the *Annotated Human Factors Taxonomy* (AHFT) which was to be used by casualty investigators as a basis for identifying human factors in marine casualties [Dynamics Research Corporation, 1989]. The AHFT is a comprehensive classification designed to assist USCG investigators in identifying and effectively recording human errors in marine casualties. The AHFT was subsequently replaced by a simpler (yet not as detailed) *Marine Casualty Human Factors Supplement* to be incorporated into a similar investigative format as CASMAIN (see Sections 2.1.2.1 and 2.1.2.2).

In the framework of error types and tokens discussed by Reason (1992), the AHFT primarily addresses error tokens. The HOE classification will incorporate factors from the front-line operator to top-level management (error types and tokens). Error tokens provide a basis for determining the underlying error types. For example, a lack of operator interest (error type) in safety contributes to insufficient tanker manning (an error token). The current status of accident data primarily focuses on active (initiating) errors with little or no information on underlying or contributing error types.

The development of HOE model framework analyses are through the examination of post-mortem studies (e.g. *Exxon Valdez* and *Piper Alpha*), and case studies (tanker loading/discharge and platform crane operations. See Chapter 7). Analysis of post-mortem studies can directly yield the error tokens (e.g. fatigue, lack of training, or judgment error) and error types (e.g. organizational communication and top-level commitments to safety) may be implemented.

The remainder of the chapter is dedicated to the error classification and how it is categorized for HOE framework modeling. The AHFT and MCHF are the bases for the HOE project

taxonomy due to their general acceptance in the marine industry. Both the AHFT and MCHF are limited in some aspects and are supplemented by the addition of several key measures of human and organizational behavior and performance including violations, commitments to safety, and allocations of safety resources.

3.2.1 The Basis for HOE Classification -The *Annotated Human Factors Taxonomy* (AHFT)

The primary basis for the HOE classification is the USCG *Annotated Human Factors Taxonomy* (AHFT) and the *Marine Casualty Human Factors Supplement* (MCHF). The AHFT was developed to improve upon the CASMAIN database to correlate underlying human factors contributing to marine casualties. The AHFT has been reviewed by regulators, operators, human factors experts and has gone through several revisions but was never implemented. The USCG concluded the AHFT was too difficult to implement by marine casualty investigators. As a result, he AHFT was further revised into the MCHF.

The AHFT was developed as the basis for USCG marine casualty investigative procedures. Figure 3.3 demonstrates the format for USCG marine casualty investigations. Stage I is an identification of prior and current ship operational characteristics. This stage is an analysis of the characteristics of the vessel operations with regard to operating procedure, equipment and technology, and personnel. Stage II identifies the personnel and task performance requirements and constraints. This stage is an assessment of the current level of performance potential to operate the system. Stage III is a determination of adequacy of performance.

In other words, were the personnel and/or task performance requirements sufficient to avoid the accident? Stage IV is the identification of the human factors in the accident sequence given the information provided in Stages I-III. The contributions of human factors are specifically identified and described in Stage V. The causes are differentiated into contributing and underlying causes, direct or casualty initiating errors, and compounding errors. Stage VI is the identification of corrective actions (applied safety management). The application of the AHFT is in Stages IV-V in the casualty analysis.

As shown in Figure 3.4, the AHFT differentiates errors into states and actions. The states include incentives and motivation of the organization and operating crews, the operating environment and situations, as well as information and communications. Error actions include active errors initiated by the operating crews. These active errors are lapses (memory failures) and slips (attention failures), mistakes (rule-based mistakes), and violations (routine violations). All active errors can be categorized as unsafe acts [Reason, 1992].

Human error related casualty causes are categorized into [Dynamic Research Corporation, 1989]:

(1) *Training and experience*: This refers to "the effects or impacts generated by concerns associated with inadequacies in training or experience of the ships permanent or transient crew members or that of port personnel associated with the loading, unloading, repair, or maintenance of the ship."

(2) *Behavioral*: This section concerns those actions "associated with psychological, emotional stressor and motivational related behavioral attributes or concerns."

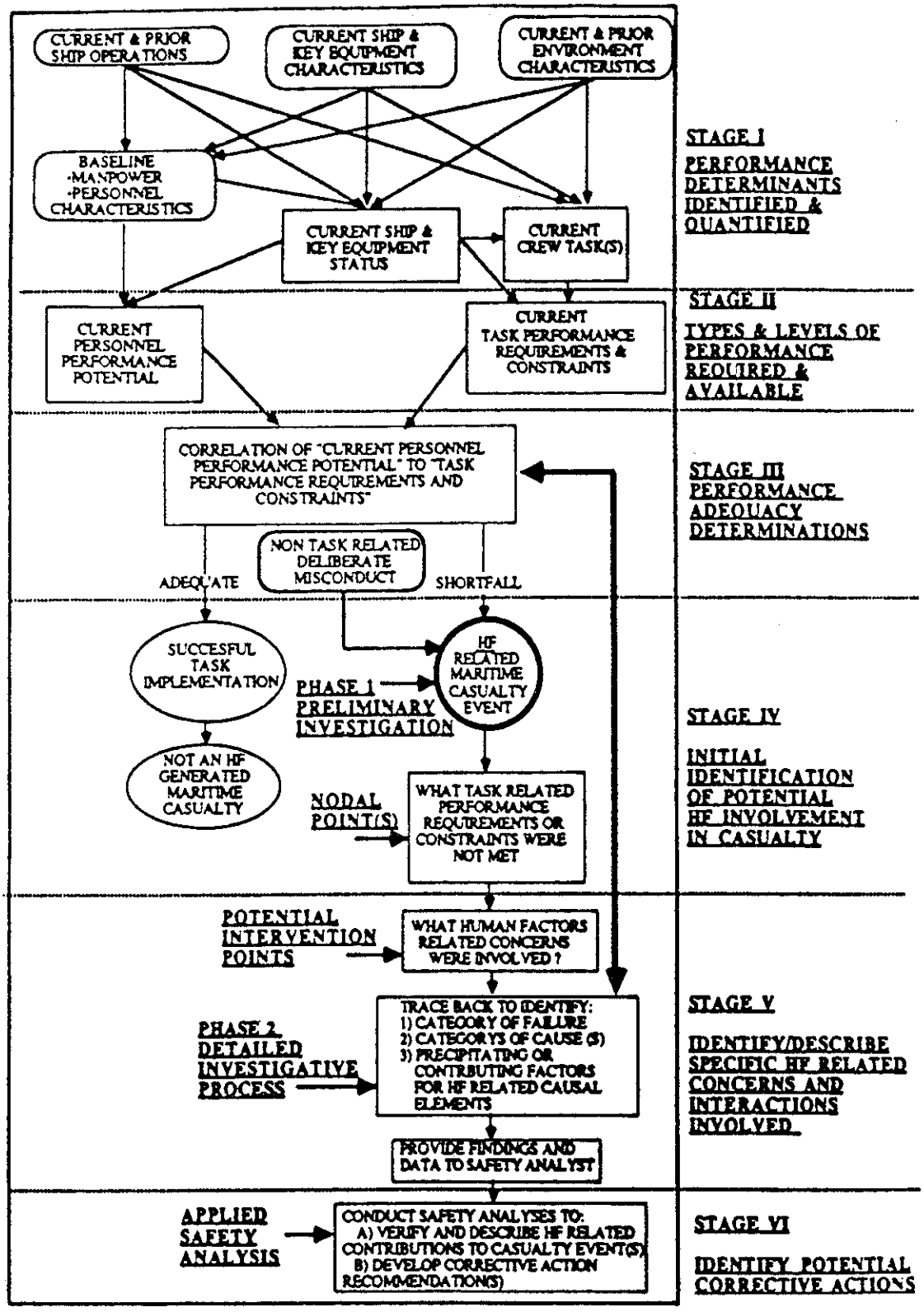


Figure 3.3 - Human factor related marine casualty investigation and safety development model [Dynamic Research Corporation, 1989]

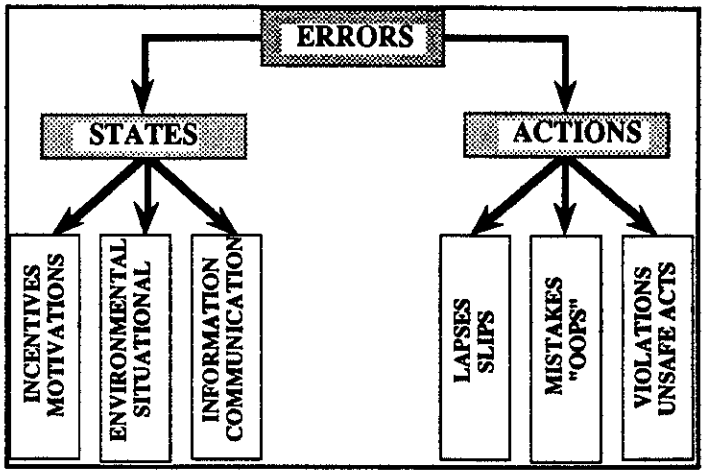


Figure 3.4 - General AHFT error breakdown

(3) *Human factors*: This topics include "all concerns associated with human intervention (action) or human engineering related to developing and sustaining the facility, equipment, software and operational interface designs needed to support the effective performance of the ships crew during normal, degraded or emergency operations and assure the health, safety, and well being of the ship's crew and passengers."

(4) *Management and administration*: This includes "all concerns associated with administrative and managerial practices that impact manpower, personnel or crew procedure or performance requirements during normal, degraded, or emergency mode operations afloat or in port."

(5) *Information/communication*: This section includes "concerns associated to any, or with any, human factor related aspect or type of transfer of significant information between crew members, ship to ship and ship to shore stations that can cause or increase the severity of a marine casualty."

(6) *Bio-medical*: This section "covers concerns any biological, physiological or medical factor capable of directly effecting the crews physical health or well being so that their ability to successfully perform their required task and/or functions, maintain good health, and/or survive is degraded to unacceptable levels."

(7) *Environment*: This heading "covers external environmental factors capable of directly or indirectly degrading human factor related concern effecting the physical, functional, operational or safety status or potential of a ship, its permanent or transient crew, passengers, or cargo in a manner or to a level that could lead to a marine casualty."

(8) *Hardware/software*: This covers "failures or shortfalls effecting a human factors related concern generated by hardware or software factors in any area of the marine operational environment that can directly or indirectly cause or increase the severity of a marine casualty."

Under each of the above error categorizations are several acronyms to describe the specific human factor. Yet the AHFT fails to capture other key elements in the human error induced casualty process:

(1) *Violations*: The AHFT makes no direct reference to violations of either the front-line operating crews, front-line management, or organization. The USCG currently maintains a separate database for violations.

(2) *Commitment to safety*: No mention is made of the influence of top-level management to the safety of the operation. Commitment to safety has two primary components: (1) motivational and, (2) resources. However, commitment to safety is not sufficient for operational reliability. There must be a competence of personnel (see "resources" below) and a cognizance of potential hazards in the operating system [Reason, 1992]. Both qualitative and quantitative models of safety commitments have been studied to determine general traits distinguishing organizations from one another [Koch, 1993].

(3) *Resources*: The commitment of resources is not only a factor of money but expertise and caliber of personnel from top-level management to front-line operators.

3.2.2 HOE Classification

The following is a presentation of the general marine operations human and organizational error classification and their descriptions. As shown in Figure 3.5, the AHFT sources lead to the following error classification.

(1) *Commitment to safety*: Commitment to safety is determined by the level of commitment of available resources (money and expertise) and cognizance of potential problems to the safety of the operational system from top-level managers to front-line operating crews. Commitment to safety encompasses humans, organizations and regulatory bodies.

There is a distinction between commitments to safety and the resources applied to the system. There can be a commitment to safety, but insufficient resources, expertise and cognizance to obtain higher levels of safety which has the effect of neutralizing the commitment to safety.

(2) *Resources*: Resources pertain to money and expertise used to heighten operational safety: Commitments of resources encompasses human tasks and performance, organizations and regulatory bodies. There may be the sufficient resources, yet little or no commitment to safety at various levels of the organization or by front-line crews. This also has an effect of neutralizing the expected commitment to safety.

(3) *Human-system interface*: Encompasses failures and shortcomings of human action resulting from inaccurate or insufficient information or from an inaccurate or insufficient response of control systems and control system display. Human/system interface problems will be addressed particularly between the front line operators and the system during normal and crisis situations.

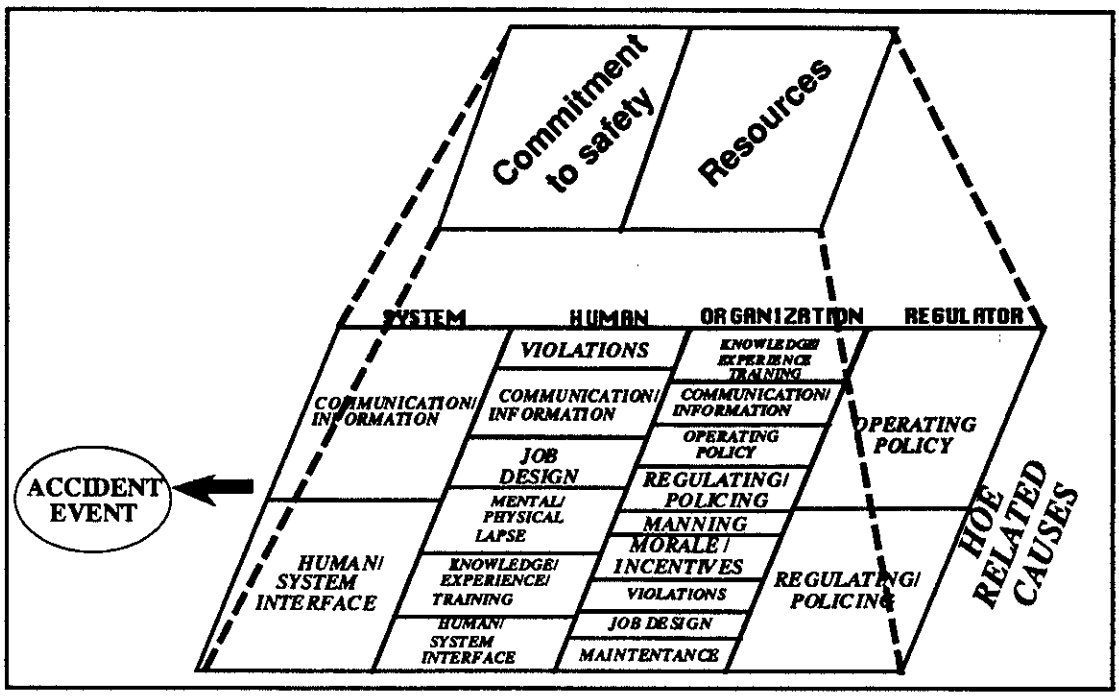


Figure 3.5 - Human and organization error classification

(4) *Knowledge/experience/training*: Pertains to human or organizational failures and shortfalls resulting from insufficient or improper knowledge, experience, or training of the system under normal or extreme operating conditions. Knowledge, experience, and training are particular issues concerning the organizations, management, and front-line operating crews responsibility of ensuring sufficient job tasks and performance level during normal and crisis situations.

(5) *Maintenance*: Refers to the impact on ship or platform operations as a result of improper, insufficient, or a failure to conduct adequate maintenance which is important to the day-to-day (normal operating systems) and extreme operating environments (safety and emergency operating systems). Maintenance is regarded to be the responsibility of the operating organization.

(6) Physical/mental lapses (including slip or mistakes): This pertains to physical or mental lapses, attention failures, memory failures, and rule based mistakes which cause or contribute to failed or inadequately manned functions or performances under normal or extreme operating conditions. The examination of physical and mental lapses, slips, and mistakes are for front-line crews whose tasks and job performances are inhibited during normal and crisis situations.

(7) *Violations*: Refers to intended unsafe acts such as routine and exceptional violations or acts of sabotage. Violations are addressed with regard to the front-line operating crews, the organizations who potentially influence the decisions and actions of the crews, and the regulatory bodies which establish the guidelines for operational policies and procedures.

(8) *Morale/incentives*: Morale refers to individual behavioral attributes that decrease the willingness, commitment and thoroughness in which individuals will conduct assigned tasks and functions. Incentives pertain to the differences in goals and preferences at different levels in the organization which lead to inadequately manned functions or performances. This examination addresses the morale and incentives of the front-line operating crews, the organizations who potentially influence the decisions and actions of the crews, and the regulatory bodies which establish the guidelines for operational policies and procedures.

(9) *Job design*: This encompasses the inappropriate match of personnel characteristics with job, task or role requirements, or inadequate job descriptions that cause and contributes to failed or inadequately manned functions and performances. Job design applies to the inappropriate match of individuals, the operational policies or procedures leading to inappropriate match of personnel, and regulatory policies which contribute to an accident scenario.

(10) *Regulating/policing*: Refers to the insufficient, inaccurate regulatory and policy making system or failure of organizations and regulatory bodies in continually maintaining or monitoring the integrity and reliability of the operating system. Regulating and policing addresses the insufficient active participation of the organization or regulatory body in maintaining the safety of the operating system.

(11) *Operating policy*: Pertains to organizational policies and procedures from top-level to front-line management which are conducive to the implementation of safety of the operating system.

(12) *Communication/nformation*: Refers to the incorrect, incomplete, or failure of the transfer of information between individuals, organizations, regulators, and systems which inhibit the safety of the operating system. Insufficient communication and transfer of information can be between human and system, or between individuals and parties on the organizational and regulatory level (i.e. top-level management, middle management, and operators).

(13) *Manning*: This embodies the inadequate manning (expertise or number of individuals) required that causes or contributes to failed or inadequately manned function or performance of the operational system. Manning decisions are maintained at the organizational and regulatory levels.

3.2.3 The External Operating Environments

The AHFT makes a distinction between error states and actions (see Figure 3.4) which contribute to accident scenarios. As shown in Figure 3.6, the HOE classification makes a further distinction between operating conditions (man-made or environmental) and error causes. The reason for this distinction is to eventually examine the effects of external operating environments on error events and causes at the various stages in an accident sequence (see Figure 3.9).

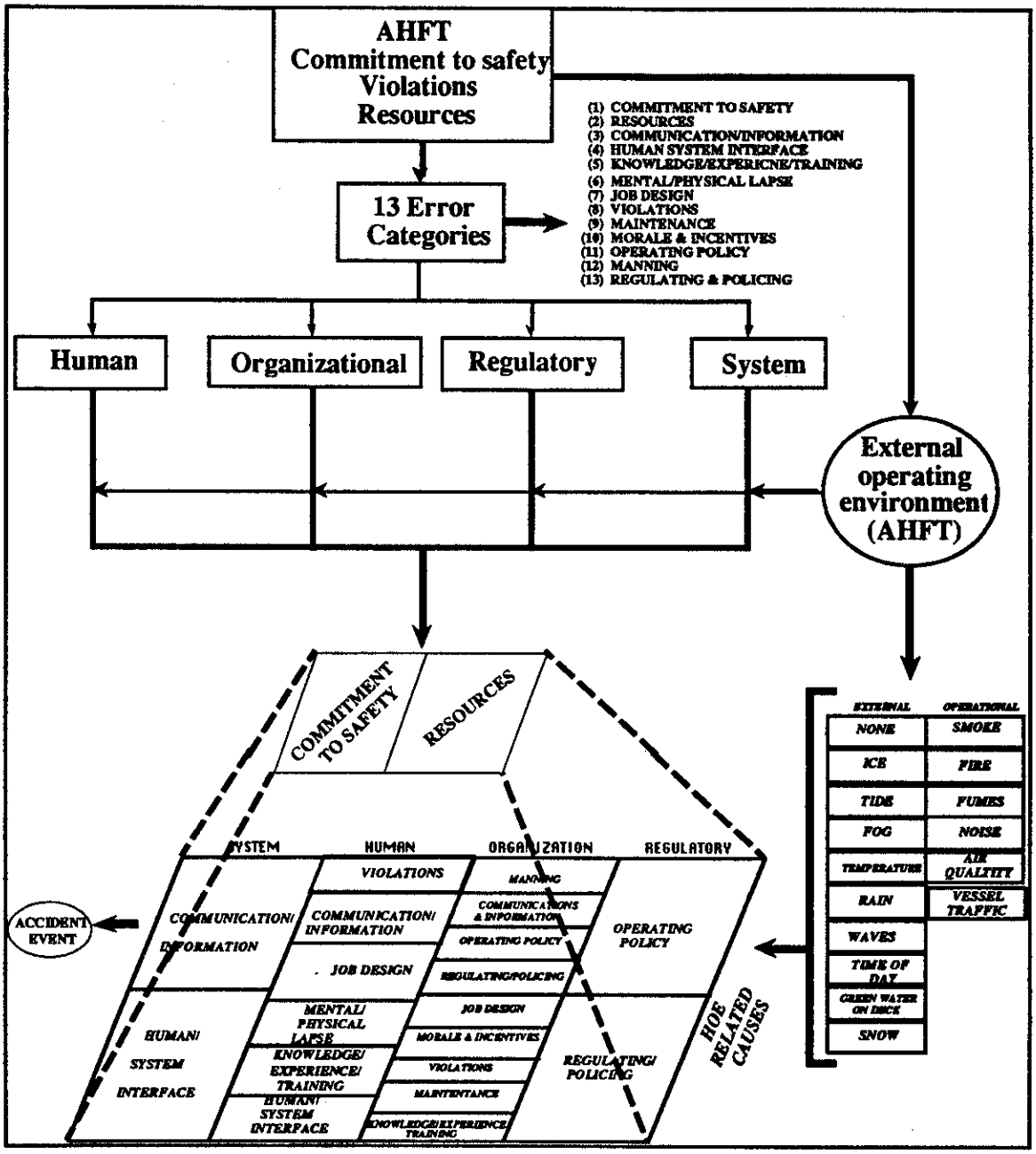


Figure 3.6 - Breakdown of AHFT taxonomy

Table 3.1 displays the categories of the *external operating environment* which are differentiated into *external* and *operational* factors. Operational factors are specific to the operating environment. The external operating environment may contribute to events, decisions, actions, or human errors. External factors pertain to the external environment (e.g. cold, snow, ice, etc.).

3.2.4 Underlying, Direct and Compounding Errors

As shown in Figures 3.7 and 3.8 we establish three stages of contributing causes to accident scenarios:

(1) *Underlying/contributing causes* represent latent errors in technology, organizational management, regulation, or immediate underlying causes for the specific error events.

(2) *Direct causes* are accident initiating errors (active errors) by front-line crews which directly effect the primary accident event.

(3) *Compounding causes* (latent errors in organizations, regulations, technological systems which enhance the casualty factors).

For example, Figures 3.7 and 3.8 demonstrate the basic events of a potential tanker grounding and a platform gas production fire respectively. Each of the events is influenced by particular HOE factors. Figure 3.7 shows the three primary events of a vessel grounding: (1) the vessel deviates from the pre-determined traffic separation scheme (underlying or contributing event), (2) the vessel runs aground (direct event), and (3) the vessel is withdrawn from the rocks after the grounding (compounding event). Similarly, Figure 3.8 demonstrates the primary events surrounding the loss of life and platform: (1) decision to conduct maintenance and production simultaneously (underlying or contributing event), (2) explosions and fires (direct event), and (3) loss of life and platform (compounding event).

Figure 3.9 is a further illustration of how human and environmental factors are organized for each stage of the accident scenario (see Figures 7.1 and 7.6). Figure 3.9 assists in determining the critical human error contributors (decision or action by the individual) to casualty events for both post-mortem studies and current operations by addressing the casualty at each relevant stage. Chapter 4 discusses in detail how this diagram is used to assist in identifying contributing HOE factors.

Table 3.1 - Classification of environmental operating conditions which contribute to HOE

External	Operational
None	*None*
Ice	*Smoke*
Waves	*Fire*
Time of day	*Fumes*
Tide	*Noise*
Fog	*Air quality*
Temperature	*Vessel traffic*
Rain	*Vibration*
Green water on deck	
Snow	
Wind	

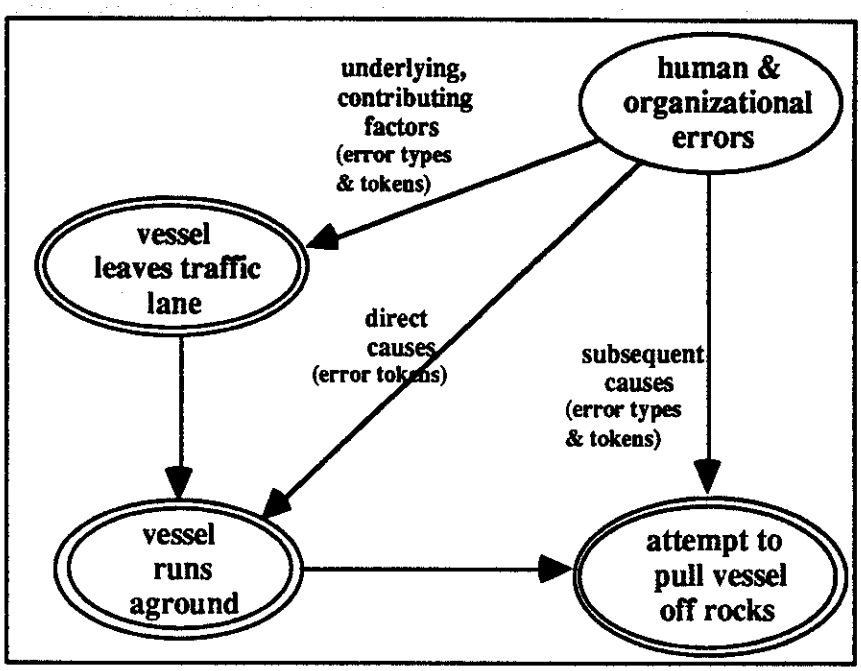


Figure 3.7 -Accident event dependencies on HOE factors for tanker grounding

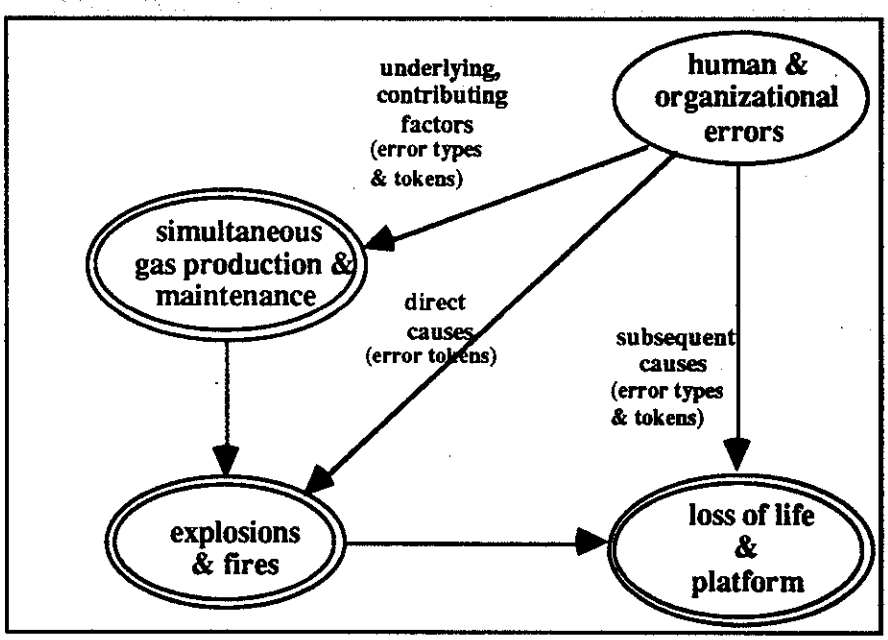


Figure 3.8 -Accident events dependencies on HOE factors for production platform gas fire

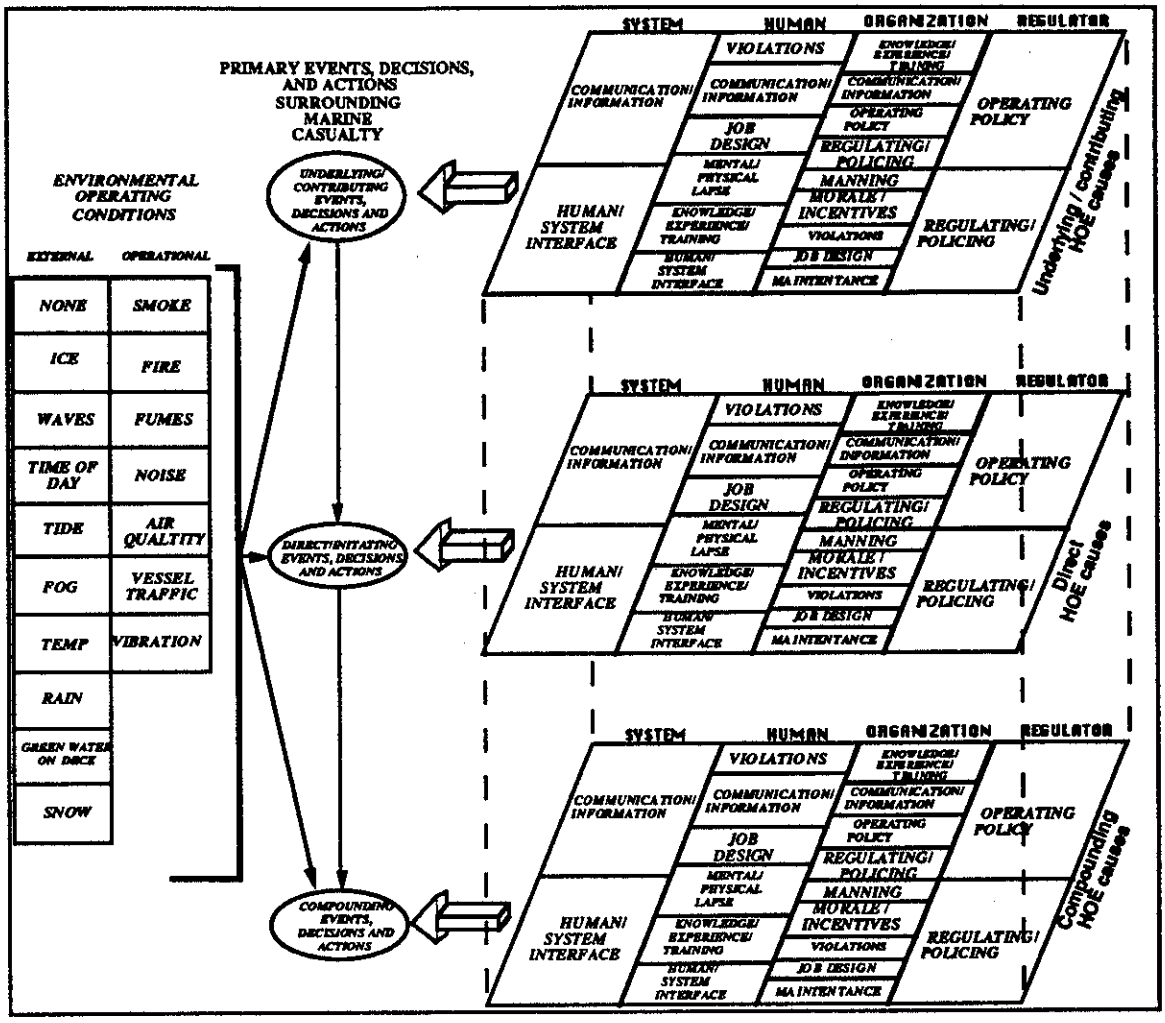


Figure 3.9 - Influence of HOEs and operating environments on marine casualty events, decisions, and actions

3.3 SUMMARY

In this chapter, a practical human and organizational error classification was developed using existing marine casualty investigation reports, databases, and error classifications. The HOE classification incorporates the proposed error classification, the USCG's AHFT, and was supplemented by the addition of several key standards by which measures of human and organizational behavior and performance including violations, commitments to safety, and allocations of safety resources are identified.

CHAPTER 4

FRAMEWORKS FOR HOE MODEL DEVELOPMENT

This chapter discusses the development of a general analytical framework based on real-life case histories of major marine casualties to characterize how the HOEs interact to cause accidents. The case histories, both post-mortem studies and currently existing operations form the basis from which accident characteristics are modeled.

Influence diagrams are used to provide the basic analytical framework to produce simplified and generalized "templates" for tanker and offshore operations that preserve the central causative mechanisms. The models are not created to predict a particular accident sequence, but to describe a general set of accident factors. For post-mortem studies, the models do not preserve the unique aspects of the particular disaster. Models of currently existing operations are developed from knowledge and experience to construct potential casualty scenarios. The influence diagram templates provide a basis in which the user may view the dependencies of contributing factors to marine related casualties though no quantitative assessments are made. The influence diagrams force the user to think in detail about important decisions, uncertainties, and interrelationships [McNamee and Celona, 1990].

In Chapter 7, these methodologies are applied to two well-documented case studies: the grounding of *Exxon Valdez* and the *Piper Alpha* disaster. The models are used as a framework to construct general models for two classes of marine casualties: (1) tanker grounding or collisions, and (2) platforms process leaks resulting from simultaneous production and maintenance. The next stage in developing analytical frameworks for HOE analyses in marine operations, is to construct influence diagram models from currently existing tanker and offshore operations. Two marine system operations were identified by the project sponsors for HOE model development: loading and discharge of tankers and crane operations for offshore platforms.

4.1 MODELING A SIMPLE MISHAP

As an introduction, a general diagram for modeling a mishap allows the user to examine a general error process from initiation to correction. Figure 4.1 provides a schematic description of a simple mishap. Once a mishap has been initiated, the objective is to return the system to normal before it reaches a critical threshold.

A mishap is differentiated into three psychological factors: *perceiving*, *thinking*, and *acting*. The danger threshold could be reached by either a lack of sufficient time to react, or errors in perception, thought or action which would either lengthen the time between events or increase the magnitude of the danger buildup. The perception stage starts with a mishap and is followed by a warning signal (see Figure 5). The warning is then noticed and leads to recognition of the mishap source. The thinking stage begins with the identification of the problem and information (whether complete or incomplete) is processed at this stage to evaluate decisions for the best course of action. The mishap is acted upon by the execution of a plan and the system is returned to a normal operating status or escalates to a dangerous state. This may be the result of an inadequately

executed plan, inadequate plan, or failure to accurately move through the necessary stages to return the operation to a normal state.

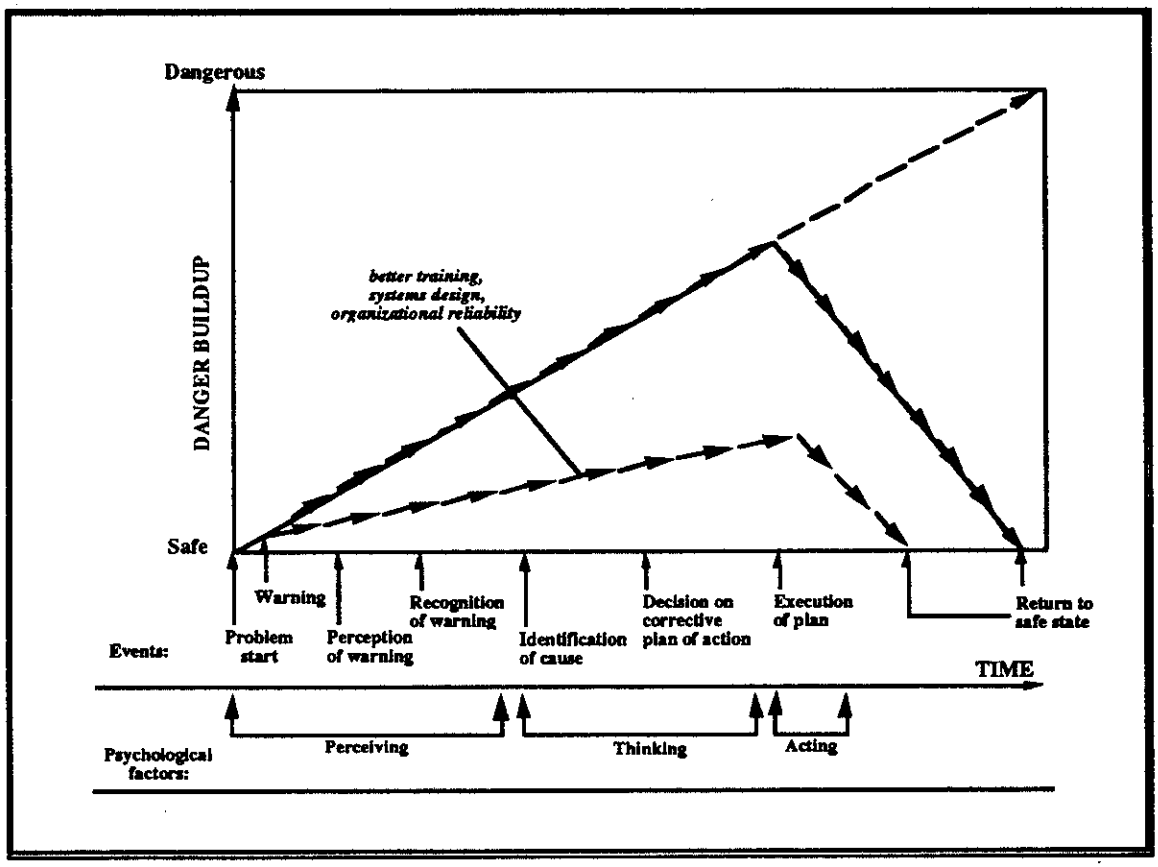


Figure 4.1 - A simple model of a mishap

4.2 CONSTRUCTING HOE MODEL TEMPLATES

One of the keys to the development of an effective model framework is to determine the goals and preferences of the user. For example, tanker or offshore platform operators may wish to establish models that enable them to focus on specific areas to allocate limited resources. These goals and preferences may be established in the model to examine the effects of the operating alternatives by weighing safety, economic, and production costs and benefits. On the other hand, regulators and policy makers may wish to establish environmental, economic and social risks and costs of specific tanker and offshore operations. In short, the models would vary to project the preferences of the user in examining costs and benefits of these operations.

The complexity of the model must be weighed against the time, available resources, goals and preferences of the user. A primary issue in model development is striking a balance between developing a general or detailed examination of specific operations. A common problem associated with structuring decision analysis models are developing inaccurate models or structuring a simple problem in a complicated manner [McNamee and Celona, 1990]. Users must ask themselves if the marginal value of information gained, as the model being constructed becomes more complex, is worth the additional input of resources. For example, the user may wish to establish a general framework model with

only limited detail and spend more time on analyzing and examining the effects of sensitivity and uncertainty in the model. Yet another individual or group may wish to develop a detailed model at a substantial cost in time and resources that allows the user to examine detailed aspects of human performance and reduce the uncertainty in the model.

In any event, the models do not particularly need to depict the real world but allow the user to differentiate between decision alternatives [McNamee and Celona, 1990]. Regardless of the level of detail the user may wish to include, each model begins with a *template* diagram which forms a basis for a specific operation. The template is a diagram involving the most relevant factors affecting a class of accidents or specific operation. The structure of the model should be shown to key players in the operation (managers, front line operators, regulators, consultants, etc.) to discuss whether the models are consistent with their judgments and experiences [Phillips, *et al.*, 1990; Swain and Guttmann, 1983]. Input from only one group may limit the effectiveness of the outcome (see communication discussion in Chapter 1). The key players should have a commitment to safety and their safety management system to make intelligent judgments [American Institute of Chemical Engineers, 1989; Gale, 1993]. Influence diagrams are an excellent source from which to understand the differences among experts viewing the same problem [Ashley, 1992]. If results are not consistent with case history examples, experience or available quantitative measures, further refinements are made.

There is a choice between encoding uncertainties or modeling the problem further [Spetzler and Staël von Holstein, 1972]. A fully descriptive model of the dynamic nature of human performance is not necessary for PRA modeling. It is impossible to fully describe all aspects of human characteristics and behavior. We now define how the human operator is described in modeling procedure. The human related components of PRA models are defined as *human reliability analysis* (HRA) and described by Swain and Guttmann (1983) as:

> "*...the probability of successful performance of the human activities necessary for either a reliable or an available system, specifically, the probability that a system-required human action, task, or job will be completed successfully within a required time period, as well as the probability that no extraneous human action detrimental to system reliability or availability will be performed.*"

Thus, one creates generally descriptive models of human factors as a component of "man-machine" systems to examine human performances directly related to casualty events.

4.2.1 Establishing Frameworks for Classes of Accident Models

A fully descriptive model of the dynamic nature of human performance is not necessary for PRA modeling [Swain and Guttmann, 1983]. Since it is impossible to fully describe all aspects of human characteristics and behavior in a PRA mode, therefore, one creates generally descriptive models of humans as components of "man-machine" systems.

Figure 1.2 provides a schematic description of the structure of this integration model. The first phase (which does not appear in this diagram) is a preliminary *quantitative risk analysis* (QRA) which identify the key subsystems or elements of the system's reliability. The modeling effort is most effective if starting with a "gross" representation (template) and refines the model with the addition of further information [Spetzler and Staël von Holstein, 1972]. The second phase is an analysis of the process to identify the potential problems for each of the subsystems and their probabilities or base rates per time unit or per operation.

Given that a basic error occurs, the next phase is an analysis of the organizational procedures and incentive system to determine their influence on the occurrence of basic errors and the probability that they are observed, recognized, communicated, and corrected in time (i.e., before a system failure event).

A basis for developing accident model frameworks was proposed by Paté-Cornell (1992). The risk analysis model is extended to include relevant decisions, actions and organizational features in risk assessment and risk management. Figure 4.2 is a hierarchical representation of the root causes behind systems failures. The primary level represents basic events affected by decisions and actions influenced by organizational policy, procedure and culture. This procedure requires the user(s) to establish an exhaustive set of contributing events and determine relevant decisions and actions specific to the class of accidents (explosions, fires, grounding, collisions, etc.).

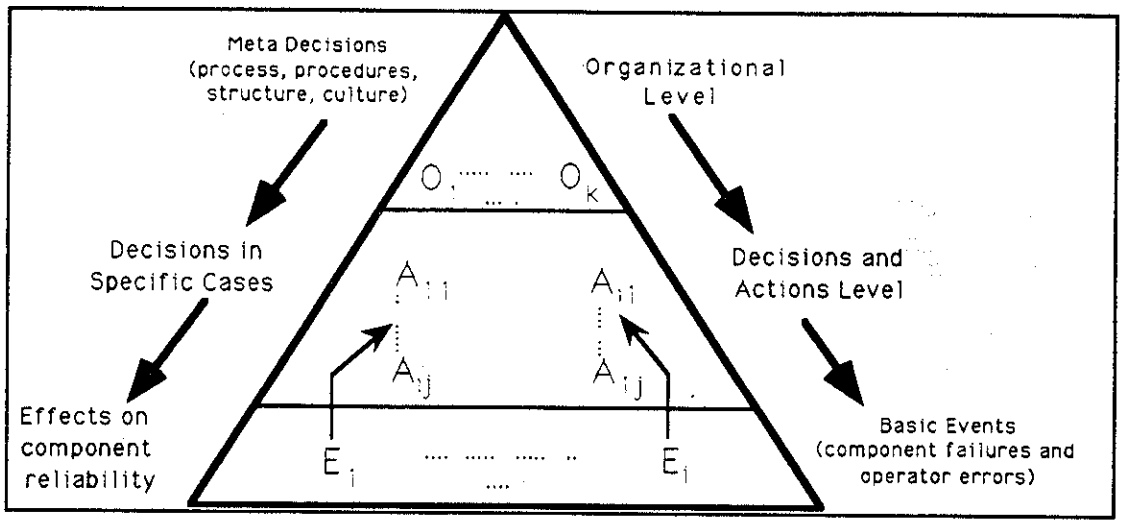


Figure 4.2 - Hierarchy of root causes of system failures - Management decisions, human errors, and component failures [Paté-Cornell, 1992]

A probabilistic model of this process includes determining the set of possible initiating accident events (in_i) and final states ($fist_m$) of the system. The probability of loss of components (platform, vessel, revenue, life, injury, etc.) to the system can then be represented by:

$$p(loss_k) = \sum_i \sum_m p(in_i)\, p(fist_m|in_i)\, p(loss_k|fist_m) \qquad \forall\, k. \tag{4.1}$$

(" $\forall$k : *for all values of k*")

The model is expanded to include relevant decisions and actions (A_n) constituting an exhaustive and mutually exclusive set of decisions or actions at different stages during the lifetime of the vessel or platform. These decisions and actions can be examined from the front-line operating crew level through to top-level management.

$$p(loss_k) = \sum_i \sum_m \sum_n p(A_n)\, p(in_i|A_n)\, p(fist_m|in_i, A_n)\, p(loss_k|fist_m, A_n) \quad \forall\, k. \tag{4.2}$$

The effects of organizational procedures and policies on the risk are determined through examining the probabilities of the actions and decisions conditioned on relevant organizational factors (O_h). The probabilities of various degrees of loss can be examined conditioned upon different contributing organizational factors.

$$p(loss_k|O_h) = \sum_i \sum_m \sum_n p(A_n|O_h)\, p(in_i|A_n)\, p(fist_m|in_i, A_n)\, p(loss_k|fist_m, A_n) \qquad (4.3)$$

4.2.2 Influence Diagrams[1]

One method of developing accident framework models for QRA analysis is through the use of *influence diagrams*. Influence diagramming is a form of QRA modeling which allows great flexibility in examining HOE and HOE management alternatives. There are distinct advantage for using influence diagrams as an alternative to standard event-fault tree analyses. In standard decision tree analysis, decisions are based on all preceding aleotory and decision variables [Howard and Matheson, 1981]. However, all information is necessarily available to a decision maker. In addition, information may come from indirect sources or may not come in the specific order in which the decision tree is modeled. It is not necessary for all nodes to be ordered in an influence diagram. This flexibility allows for decision makers who agree on common based states of information, but differ in ability to observe certain variables in the diagram modeling [Howard and Matheson, 1981]. Influence diagrams are able to organize conditional probability assessments required to determine unconditional probabilities of failures of specified target events [Phillips, *et al.*, 1990].

As described by Howard (1990), the components of an influence diagram are: (1) *decision* and *chance nodes*, (2) *arrows*, (3) *deterministic nodes*, and (4) *value nodes*. As shown in Figure 4.3, decisions are represented by square nodes which can be a continuous or discrete variable or a set of decision alternatives. Uncertain events or variables are represented by circular or oval chance nodes. Chance nodes can be continuous or discrete random variables or a set of events. Arrows indicate relationships between nodes in the diagram. Arrows entering a chance node signify that the probability assignments of the node are conditional upon the node from which the arrow originated. Deterministic nodes are those in which outcomes depend deterministically upon its predecessors. A value node is designated by the author to be: "the quantity whose certain equivalent is to be optimized by the decisions" of which only one node may be designated in the diagram. Value nodes may be a distribution of possible values. This is represented by a rounded edge single-border node. The value node may also be represented as the expected value. These nodes are represented by a rounded edge double-border rectangle.

---

[1] The *influence diagram* is defined by Bodily (1985) as:

> *"...a display of all of the decisions, intermediate variables, outcome attributes that pertain to a problem, along with the influence relationships among them. By influence we mean a dependency of a variable on the level of another variable."*

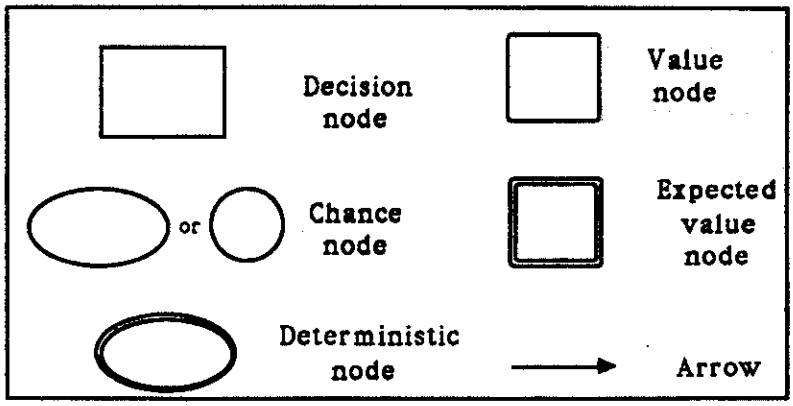


Figure 4.3 - Influence diagram characterizations

4.2.2.1 Using Influence Diagram Modeling Methods - The Decision Analysis Cycle
Figure 4.4, describes the process through which decision analysis models are developed. This process is described as the *decision analysis cycle* and is generally described in similar fashion in a number of decision analysis related literature [Spetzler and Staël von Holstein, 1972; Howard and Matheson, 1981; McNamee and Celona, 1990]. The four general phases are the: (1) *deterministic phase*, (2) *probabilistic phase*, (3) *information phase*, and (4) *information gathering phase*.

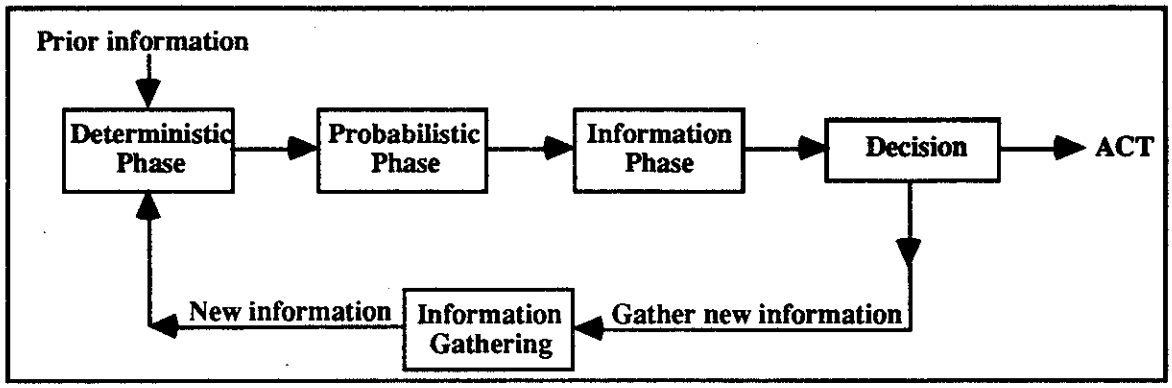


Figure 4.4 - The decision analysis cycle [Howard and Matheson, 1981]

The deterministic phase is where variables affecting the decisions are defined and related. This phase is devoted to establishing influences (dependencies) between variables, qualitative structuring of the system, and assigning appropriate outcomes. This phase is dedicated to structuring framework models, collecting pertinent data, and ranking the importance of variables without consideration being made of their uncertainties. The decision makers in the potential scenarios should be present in the modeling process since they are more able to truly distinguish the decision alternatives available to the operator.

As exemplified in Chapter 7, preliminary models representing accident scenarios (influence diagram representations discussed in Section 4.3 and case studies shown in Figures 7.3 and 7.7) are constructed to highlight particularly events, decisions, actions, or errors contributing to the accident scenario. The models are further reduced into templates which preserve the causative mechanisms of the accidents but are not

particularly complicated. This process is carried out through two methods: elimination through judgment or experience and sensitivity analysis.

Eliminating contributing factors through judgment or experience involves understanding the system and what factors are primary contributors to an accident scenario. Not every "failure path" for an accident sequence may be studied leaving it to the discretion of the user to make valuable judgments as to what should be deleted. On the other hand, sensitivity analysis is a method which allows the user to subjectively quantify the sensitivity of a variable to determine it's importance to the model (sensitivity analysis is discussed in Chapter 5). The modeling procedure used for the deterministic phase are discussed for post-mortem studies (see Section 4.3) and existing operations (see Section 4.4).

The probabilistic phase, discussed in Chapter 5, is the introduction of probability assignments to variables and values. As discussed in Chapter 3, the lack of available data has left us to making heuristic judgments for the probabilities of contributing factors to marine casualties. A number of methods of arriving at quantitative measurements of accident contributing factors are discussed in Chapter 5. In addition, a methodology is developed for collection of HOE data which incorporates human, organizational, system, and environmental factors (see Section 5.5).

The information phase is devoted to determining whether the acquisition of additional information is beneficial to the user. We establish the value of information by placing a value upon additional information that would reduce the uncertainty of the model. If the value of new information is beneficial, then alternatives should be reviewed to acquire the additional information. This initiates the information gathering procedure. Alternatives for acquisition of the new information must be taken into account as well as potential impacts of delaying decisions by further modeling. The information phase is discussed further in Chapter 6.

4.3 DEVELOPING ACCIDENT FRAMEWORK MODELS FROM POST-MORTEM STUDIES

As mentioned in Chapter 3, the use of post-mortem studies as a source of information to construct accident model frameworks have both advantages and disadvantages. This chapter discusses a systematic method in which to model specific HOE related events, decisions, and actions which are used to formulate models of classes of marine accidents from post-mortem studies. Chapters 7 further develops the modeling framework using the *Exxon Valdez* and *Piper Alpha* disasters as case study examples.

Chapter 3 discussed the levels at which safety information data is obtained and analyzed. Accident and incident reports (post-mortem studies) are the most commonly available and used data sources for tanker and offshore platform operations. Figure 3.2 shows the levels of safety information from examination of both error types and tokens [Reason, 1992] (see discussion on error types and tokens, Chapter 3). Nevertheless, human and organizational errors through post-mortem analyses have both advantages and drawbacks that are both qualitative (examination of accident sequences, investigative biases, etc.) and quantitative (e.g. probabilistic updating of system failure rates) in nature. This leads to the conclusion of the importance in integrating case study knowledge (accident trends in case study analyses) with theories of the nature of the underlying causes and related accident events (assessing contributing causes in accident trends).

posterior distributions of parameters leading to accident events [Oliver and Yang, 1990].

(4) *Unintentional flaws in reconstructing history creates "hindsight bias"* [Ashley, 1992]. Hindsight bias tends to take focus away from risks which may have previously been identified, well documented, and itemized. Case histories can inadvertently prepare one to not deal with new events which were not previously encountered.

4.3.3 Methodology for Model Development - Post-Mortem Studies

Four principle steps are involved in the development of a post-mortem study model: (1) structure the relevant events, decisions, and actions specific to the accident scenario, (2) apply human and organizational error classifications to identify contributing HOE factors, (3) develop a model representative of a "class of accidents" of which the post-mortem case study was related, and (4) determine a general set of contributing HOE causes related to actions, decisions and events leading to the particular class of accidents.

4.3.3.1 Structuring Relevant Events, Decisions and Actions - An Influence Diagram Representation for Post-Mortem Studies

In general, there are two types of input variables for the modeling procedure: *decisions* and *state* variables. Decisions are variables in which the decision maker has control and state variables are those over which the decision maker has no control. To establish the set of events which have occurred in a specific accident sequence, the user may wish to construct a preliminary influence diagram representation of the accident. The preliminary model representation is not an influence diagram per se, but a representation of the specific events, actions, and decisions which occurred during the accident event. The purpose of the preliminary model is to assist the user in establishing the relevant contributing factors unique to the specific accident sequence [see Figure 7.3 and Figure 7.7]. No quantitative assessments are made from the preliminary model. In addition, it can assist the user in identifying critical areas where: (1) further detailed studies may be warranted, or (2) categories where risk or consequences of the accident may be avoided or mitigated.

As shown in Figure 4.5, the modeling process begins with a specific accident model formulation and results in the development of an influence diagram model for a particular class of accidents. The influence diagram models encompass the class of accidents in which the post-mortem model is a representative. The development of influence diagram models (and preliminary model representations) should be the effort of a group of experts who are knowledgeable in the specific areas of operation. Differences in opinion of relationships between events and their causes should illicit discussion to assist in generating realistic models [Phillips, *et al.*, 1990]. The models are developed through an iterative process discussed between experts to determine relevant influences and correlation between subsystems and operations.

The modeling process follows the same methodology discussed by Paté-Cornell (1992) in Section 4.2.1. This includes the structuring of a target event (e.g. platform fire, vessel grounding, etc.) which is the final result of contributing events, decisions, and actions. The first step is to develop a model representing dependencies between relevant events. Events can be categorized into three stages:

4.3.1 Advantages of Using Post-Mortem Studies for HOE Analyses

The importance of post-mortem studies in marine casualty studies are the following:

(1) *Intensive studies of a single case can reveal the influences and correlation of underlying and contributing, direct, and compounding causes to a complex set of accident events over time* [Reason, 1990; Swaton and Tolstykh, 1990]. Case studies are a tool to examine prevailing circumstances and conditions (environment or operational) unique to a specific accident scenario which may otherwise be difficult to capture (*20/20* hindsight).

(2) *Post-mortem studies may reveal classes of accident causing factors or scenarios which may have been latent or overlooked* [Paté-Cornell, 1992]. For example, the complex interactions of causes and events surrounding the *Piper Alpha* disaster could have easily been overlooked or suggested to be so remote so as to be disregarded as a potential accident scenario. Post-mortem studies of *Piper Alpha* have revealed many of the sub-system failures not otherwise noticed [Paté-Cornell, 1992; Institute of Marine Engineers, 1991; United Kingdom Department of Energy, 1988, 1989, 1990].

(3) *Post mortem studies provide valuable information for probabilistic updating of system failure rates conditional upon human, organizational, conditional and prevailing contributing factors* [Paté-Cornell, 1992; Swaton and Tolstykh, 1990]. Bayesian updating (conditional probabilities) is an important quantitative component to the analysis of overall failure rates of the systems in light of the scarcity of accident and incident data in the marine industry [Bea and Moore, 1991; Laroque and Mudan, 1982].

4.3.2 Drawbacks of Using Post-Mortem Studies for HOE Analyses

Though post-mortem studies provide valuable insight into examining HOE in marine casualties, the following limitations exist:

(1) *Post-mortem studies do not capture all factors involved in an accident or incident sequence* [Reason, 1990] (see Section 2.1.1).

(2) *Many accident reports primarily focus on attributing blame* [Reason, 1990; Paté-Cornell, 1992]. Marine casualty investigations should not be directed at assessing blame, but focus on providing greater insight into the interactions between circumstances, events, decisions, and causes of HOE. Catastrophic marine casualties are the accumulation of compounded factors contributed by parties across organizational levels over an extended period of time. Assessing blame tends to draw focus away from the primary goal of determining HOE management alternatives through reducing risks and/or consequences of a marine operating system.

(3) *Focus on determining the probability of failure of a unique set of circumstances surrounding an accident after the fact can lead to inaccurate assessments of risk* [Paté-Cornell, 1992]. Low probability-high consequence technologies are statistically vulnerable to low probability estimates of system failures [Freudenburg, 1988]. Post-mortem study analyses should focus on probabilistic modeling and assessments of "classes" of accidents, not on cause and event sequences unique to a specified documented case study given the lack of specific patterns and trends [Reason, 1992]. Though, the analyses of series of post-mortem studies can lead to insight into accident trends and error management alternatives. There is currently no formal updating scheme in which historical data of particular accident sequences are used to obtain

(1) *Contributing-underlying events*: An event that contributes to the reduction of reliability or increase of risk for the system. For example, a tanker departing from a traffic separation scheme (*Exxon Valdez*) or an offshore platform producing and conducting production process maintenance simultaneously (*Piper Alpha*).

(2) *Initiating-direct accident events*: The immediate accident event(s) resulting in the casualty. For example, a tanker grounding or the initial explosions aboard a production platform subsequently lead to a compounding of events (e.g. oil spill, loss of life and platform).

(3) *Compounding events*: The progression of events which leads to compounding of accident consequences. For example, attempting to dislodge *Exxon Valdez* from Bligh Reef after grounding results in a larger spill, or increasing the flow of gas from satellite platforms *Claymore* and *Tartan* to *Piper Alpha* resulting in riser fires that compounded the catastrophe.

Examples of the influence of events in accident sequences for tanker and offshore production platform are shown in Figure 4.6. For the tanker, the underlying-contributing event is the vessel deviating from the traffic separation scheme. The initiating-direct accident event is the vessel grounding, and the compounding event is dislodging the vessel from the rocks. Similarly, a diagram representation of simultaneous production and maintenance leads to an initial explosion and consequently loss of life and platform.

The next step is to establish contributing decisions and actions influencing the set of accident events. Dependence between events, decisions and actions are represented by arrows leading from decisions and actions to relevant events (see Figures 3.7 and 3.8 for the tanker and offshore platform examples).

The final step entails expanding the diagram to include the influences of HOE factors and operating environmental conditions upon events, decisions and actions (see Figures 4.7 and 4.9). In Chapter 3, the HOE classification for addressing contributing HOE factors and environmental operating conditions has been developed. Environmental conditions (temperature, waves, smoke, fire, etc.) can potentially influence events, decisions, actions and human and organizational errors. For example, operating crews are subject to errors in communication in high noise environments (e.g. tanker engine room or platform production module).

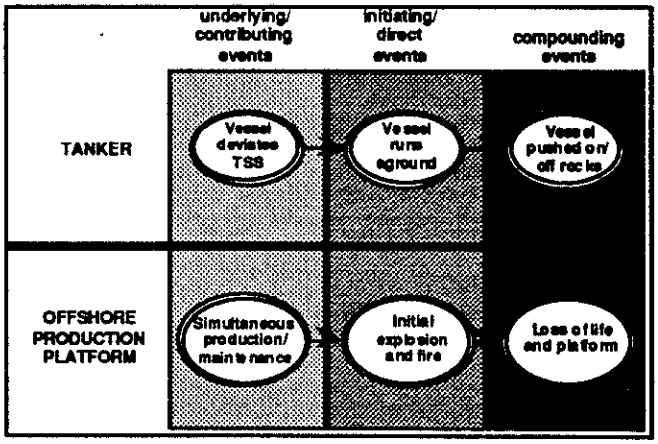


Figure 4.6 - Examples representing progression of accident events

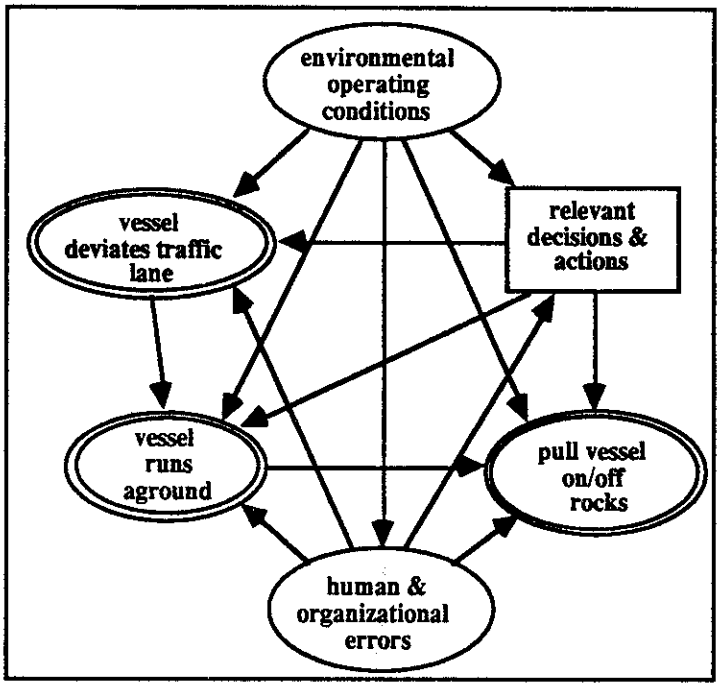


Figure 4.7 - Accident event dependencies upon relevant decisions, actions, environmental conditions, and HOE factors for tanker grounding

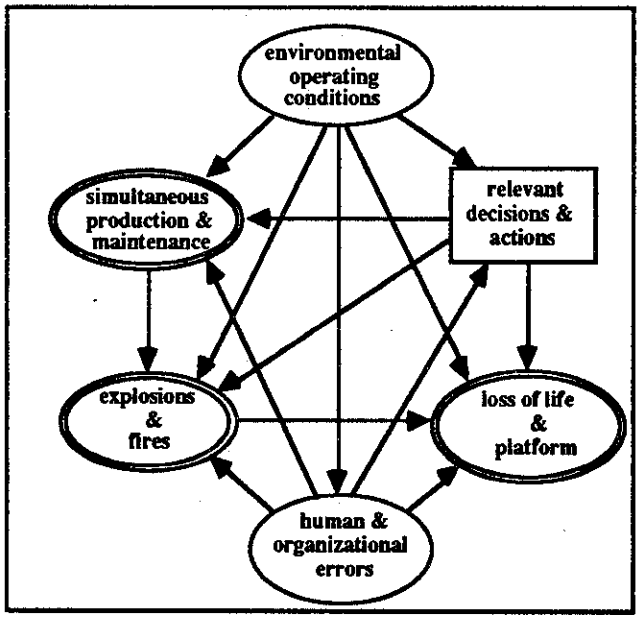


Figure 4.8 - Accident event dependencies upon relevant decisions, actions, environmental conditions, and HOE factors for simultaneous production and maintenance

4.3.3.2 Expressing HOEs and HOE contributors in influence diagrams

Human errors and contributors to human errors such as organizational errors, system complexities, human factors, and environmental factors, can be expressed either explicitly (solid arrows) or implicitly (dotted arrows) in an influence diagram. Explicit accounting of human errors and their contributors is represented by including a node for those factors within the influence diagram as shown below in Figure 4.9. One can implicitly account for human errors by excluding them from the influence diagram. But the errors are accounted for by defining what effect errors will have on operational EDAs and casualty consequences and adjusting the quantitative measurement of the EDA accordingly. The nodes with dotted arrows represent factors that can be represented by an implicit influence. Examples of both explicit and implicit accounting of human errors in the influence diagrams are provided in Chapter 7.

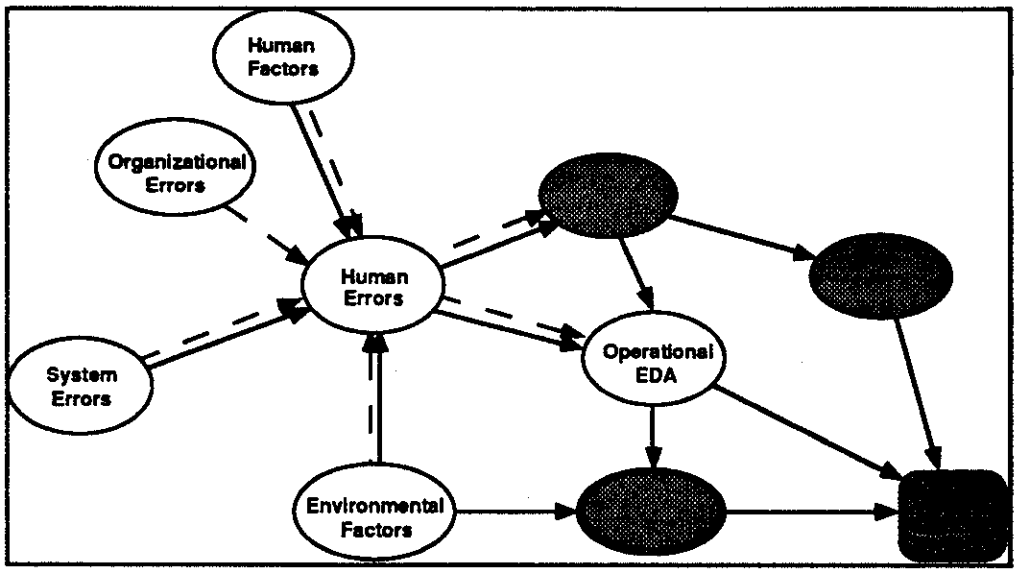


Figure 4.9 - Modeling human errors using influence diagrams

4.4 DEVELOPING ACCIDENT FRAMEWORK MODELS FOR EXISTING OPERATIONS

Similar to the post-mortem study, the structuring of template models to represent a particular class of accidents for currently existing operations is a primary goal. Model developments from currently existing operations can be the result of expert opinion, "near miss" data, particular trends in accident related events, decisions, actions, and human and organizational errors.

The study of currently existing operations requires the users to be particularly cognizant of the problems and the potential consequences. The currently existing operational models do not draw from the particular advantages of post-mortem studies as discussed in Section 4.3.1. The primary difference between the development of the currently existing operation model and the post-mortem study model is that an influence diagram model representation of specific accident sequences is not generated before templates are produced.

An initial representation of a particular accident scenario may assist the users in determining the truly critical factors in general accident trends. Modeling issues must be discussed between experts to determine realistic scenarios for accident analysis and avoid excessive detail in the modeling procedure yet incorporate the important contributing factors (see Section 4.2). A formal testing procedure of the relevance of particular contributing factors to accident scenarios are discussed in Section 5.3.4.

4.4.1 Structuring Relevant Events, Decisions, and Actions - Existing Operations
The modeling procedure follows the same particular steps of the post-mortem study of determining contributing factors. Though these factors are generated through knowledge, experience, judgment, and expertise and not from accident data. This includes the structuring of a target event (e.g. loss of life or structural integrity due to loss of control of crane load, product spill resulting from loss of fuel containment during tanker loading or discharge, etc.) which is the final result of contributing events, decisions, and actions. The first step is to develop a model representing dependencies between relevant events for existing operations. Events can be categorized into three states:

(1) *Contributing-underlying events*: Events occurring prior to the initiating accident event contributing to the reduction of reliability or increase of risk for the system. (e.g. initiation of a tanker load or discharge at an improper rate or time, or conducting offshore crane operations without proper supervision).

(2) *Initiating-direct accident events*: The immediate accident event(s) resulting in the casualty. (e.g. example, loss of fuel containment while loading or discharging a tanker or loss of control of a crane load on an offshore platform).

(3) *Compounding events*: The progression of events which lead to compounding of accident consequences (e.g. oil spill, loss of life, or platform integrity).

Examples of the influence of events on accident sequences for tanker and offshore production platform are shown in Figure 4.10. For the tanker, the underlying-contributing event is the "loading or discharge of cargo". The initiating-direct accident event is the "loss of fuel containment" during transfer, and the compounding event is a "spill in water". Similarly, a diagram representation for crane accidents represents underlying- contributing event as "initiation of crane operations", initiating-direct event is the "loss of crane load control", and the compounding event is the "loss of life, injury or platform damage". These examples are explored further in the Chapter 7.

As for the post-mortem study, the next step is to establish contributing decisions and actions influencing the set of accident events. The final step in developing the model framework entails extending the model to include the influences of HOE and operating environment factors upon events, decisions and actions. This is accomplished by integrating the influences discussed in Chapter 3 and shown in Figure 3.9. The determination of impact of HOE contribution and environmental factors are at the discretion of the user. HOE and conditions in the operating environment can affect events, decisions and actions conducted by operating crews.

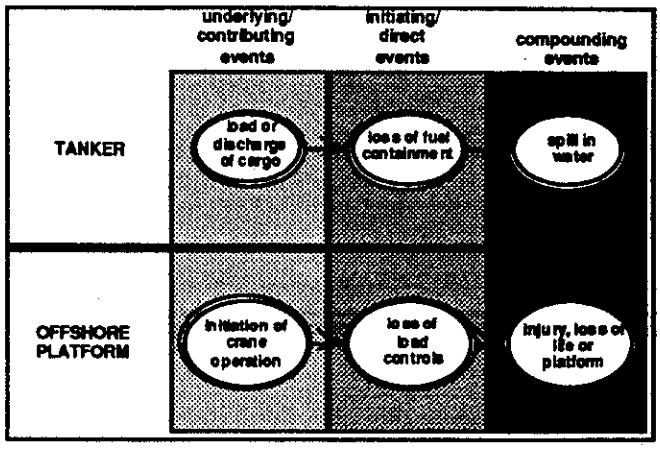


Figure 4.10 - Examples representing progression of accident events

4.5 SUMMARY

Post-mortem study models and examination of currently existing operations provide a basis on which to construct quantitative models (influence diagrams) of general classes of accidents. Analyses of post-mortem accident studies lead to a greater understanding of the effects of HOE in accident sequences. However, the relative advantages and drawbacks should be addressed by the user. Knowledge and expertise of the operating system is particularly critical for studying current operations where accident data may be scarce.

A lack of quantitative information limits assessment of conditional probabilities of accident related factors. Therefore, one must rely on expert opinion and limited data sources. Nevertheless, developments of influence diagram models assist user in determining and examining complex interactions of humans, organizations, and systems. The influence diagram templates provide a basis in which to view the interactions of contributing factors to marine related casualties event though no quantitative assessments are made. The following chapter addresses the next step in the modeling procedure: quantitative modeling.

CHAPTER 5

QUANTITATIVE RISK ANALYSIS

The objective of Task 4 of the HOE research project was to formulate quantitative models for the case histories based on quantitative risk analysis procedures. The primary steps in modeling human performance for operations of marine systems were discussed in Chapters 3 and 4. In Chapter 3 a classification of human and organizational errors was established as a basis for categorizing errors. Chapter 4 described the methodology for building models relating failure contributions to underlying, direct, and compounding events, decisions, and actions. Influence diagrams were also introduced in Chapter 4 as a means by which to develop quantitative models. The next step of the modeling procedure was to develop means by which to establish intelligent judgments for quantifying HOE. Once the quantitative values are derived, influence diagrams can be used as the quantitative modeling tool (see Section 4.2.2).

As discussed in Chapter 2, the lack of data reflecting the impacts of HOEs in marine casualties has hampered the development of quantitative models that can assist operators, managers, engineers, and regulators in developing engineering based reliability models.

Estimates for human error quantification can be obtained in three ways: (1) *historical data*, (2) *expert judgment and experience*, and (3) *experimentation and simulation*. Historic data allows for the analysis of operations under different operating conditions for marine related casualties. However, as mentioned before, the lack of historic data has hampered the abilities to perform human reliability based analyses. Expert judgment is a strong approach that allows for those familiar with the of human factors, the engineered system, operators, and other specialists to identify and assess critical factors in an operational system.

Many engineered systems have relied heavily upon expert judgment in light of the limited data available for low-probability high-consequence accidents. Expert judgments have discrepancies that affect quantitative measurements such as biases and inability to understand the impacts of latent flaws in the system or new technologies. However, in light of the lack of data, expert judgment is a strong tool for quantitative measurements. Experimentation and simulation allow for determination of error causing factors under controlled situations. Experimentation and simulation have been used in many industries such as flight operations, nuclear power, process industries, and vessels and offshore platforms. Though experimentation and simulation are helpful, they are performed in controlled environments where the operator knows he or she is being monitored and the consequences of a mishap are not catastrophic. These factors can lead to biased results.

To date, none of the current quantification procedures explicitly address the impact of organizational behavior, culture, operations, or procedures upon human errors. This lack of comprehensive HOE data is not unique to the marine industry. The problems of limited casualty data has led the nuclear power industry to introduce a number of works examining methods to quantify human error by front-line operators [American Nuclear Society and Institute of Electrical and Electronic Engineers, 1983; Bell and Swain, 1983; Oliver and Yang, 1990; Swain, 1987; Swain and Guttmann, 1983]. Each of these error analysis

methodology incorporate varied levels of expert opinion and judgment of operators, engineers, managers, and regulators familiar with the operational system being modeled.

Though there will always be a necessity for expert opinion and judgment for developing the model structures of marine operations, there is a need to reduce the dependence upon opinion and judgment to arrive at quantitative values. There are three general stages of quantifying HOE for marine operations dependent upon whether limited, marginal, or comprehensive data available. Each of these modeling techniques are described in this chapter. As shown in Figure 5.1, the first quantitative analysis procedure, *probability encoding*, relies on little or no HOE data. Heuristic judgment and experience of operators, managers, and/or regulatory agencies are used to establish reasonable estimates for accident contributing factors in absence of casualty data.

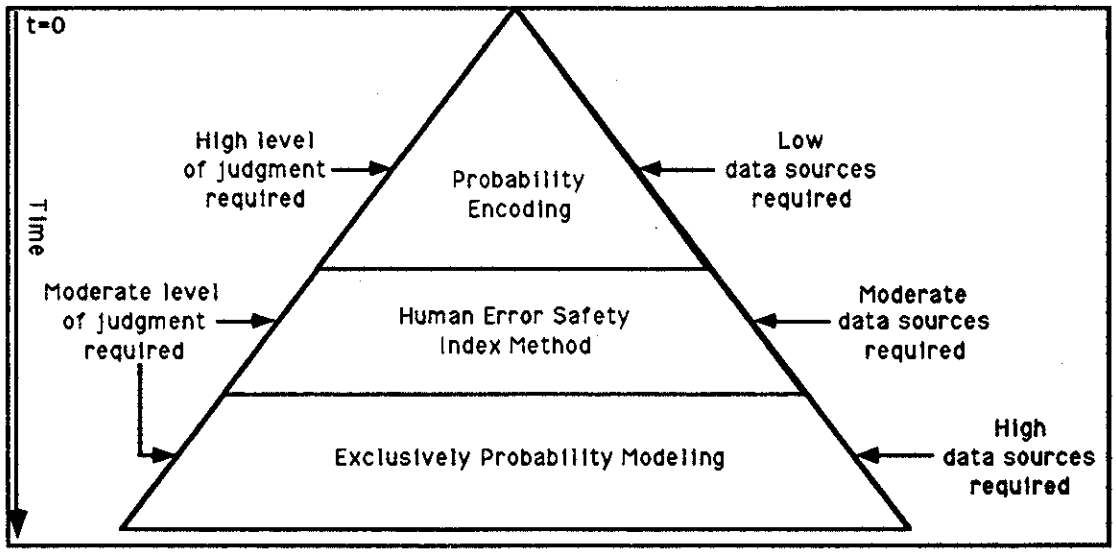


Figure 5.1 - HOE analysis types dependent upon the amount of data available

The second quantitative analysis procedure is a heuristic-probabilistic approach using an indexing method that relies upon judgment, experience, and HOE data as it becomes available (Bayesian updating). The safety index method entitled the *Human Error Safety Index Method* (HESIM) incorporates contributions of organizational, system, and environmental factors affecting human errors during operations. This approach is a systematic error quantification method used for quantitative analysis. The safety indices are used in the influence diagrams to generate risk indices for the operation of interest. The HESIM can also be used as a means from which to assess HOE management alternatives [Moore and Bea, 1993]. Updated index values are used in the influence diagrams to determine the relative effects upon the reduction of particular accident sequences.

The third procedure relies least upon extensive expert judgment and most upon the objective error data being collected. This leads to the final quantitative analysis procedure that entails providing the user with a framework from which to document and analyze accident causing factors. The database system, the *Human and Organizational Error Data and Quantification System* (HOEDQS) described in this chapter serves two purposes. First, it provides a basis from which to obtain quantitative measurements for the HESIM described in the previous section. It has been developed to incorporate the data being collected-updated the expert judgment in generating quantitative measurements for

organizational, human factors, system, and environmental contributors. Second, the database system provides the framework from which to generate HOE frequency measures for casualties and near misses. The specifics of both the HESIM and HOEDQS collection procedure are introduced in this chapter. Appendix 3 and provides a user guide to the HESIM and HOEDQS programs written on *Excel*™ v.4.0 for the Macintosh. In addition a floppy disk copies are also provided for the system.

Refinements and verification of the HESIM is required to arrive at reasonable HOE estimates. The values that are generated from the HESIM are not probabilities per se, but through this approach one is able to systematically generate error quantification indices to be used for quantitative analysis. The safety indices (risk indices) are then used in the influence diagrams to generate a risk index for the events of interest (e.g. tankship collision or grounding). A method for calibrating the safety index to the probability of failure is also proposed in this chapter.

Verification of risk index methods have been performed in some of the above mentioned operational domains [American Institute of Chemical Engineers, 1987; Bea and Craig, 1993; Hannaman, *et al.*, 1984]. Detailed case studies of tanker loading and discharge operations are to be used for verification of the HESIM in the following year [Bea and Roberts, 1993].

5.1 HISTORIC BACKGROUND OF HRA-QRA MODELING

In order to develop quantitative models to assess the impact of human and organizational errors on the operations of marine systems, two primary elements must be fulfilled. A structured modeling procedure to systematically identify human errors in potential casualty scenarios must be developed. Historically, *quantitative risk analysis* (QRA) procedures have been applied as a means by which to structure the reliability of an engineered system. Quantitative risk analyses have been used to determine failure (fault tree) or success (event tree) of sub-systems and relating these failures directly to the success or failure of the overall system. Within the last 15 years, *human reliability analysis* (HRA) has been developed as an integral part of the QRA analysis. Human reliability analysis is a QRA based modeling methodology that integrates the human element into the QRA procedure as it does for any other sub-system: as a component with a degree of success or failure.

Current QRA procedures have come under strong criticism because they do not sufficiently model humans in the failure analysis procedures. One of the discrepancies of the fault or event tree analyses used is the reliance upon conditioning of error contributors that may not have a direct effect upon a human error at a particular stage in an accident scenario.

This chapter discusses the current status of methodologies to model and quantify HOE for marine systems. The current QRA and HRA modeling methodologies are reviewed and their advantages and discrepancies are discussed. Influence diagram modeling is introduced as a modeling procedure that allows users with varying degrees of experience with QRA, a method to both qualitatively and quantitatively structure the relevant contributors to an accident scenario.

Another of the major criticisms of the QRA-HRA based procedures is the glaring lack of human error data from which to drive the models [Moore and Bea, 1993; Reason, 1990; Swain and Guttmann, 1983]. For the marine industry, this deficiency has been the result of industry culture, deficiencies in investigative procedures, legal reasons, and, foremost, a general lack of familiarity of how to properly describe the complex interactions be-

tween the human and his or her operating environment. The discrepancies of current databases from which to perform reliability based model analyses are also discussed.

5.2 QUANTITATIVE RISK ANALYSIS AND HUMAN RELIABILITY ANALYSIS

The first tools for quantifying the failures of a system was *probabilistic risk assessment* (PRA). Probabilistic risk assessment has been defined as "a rigorous and systematic identification of the levels of damage that could conceivably result from ...[a system's]... operation and the quantitative assessment of the likelihood of such occurrences" [Zion Probabilistic Safety Study, 1981]. Probabilistic risk analysis started in the nuclear power industry as a means by which to quantify risks of catastrophic failures. As described by Reason (1990) probabilistic risk analysis was a major advancement in the area of engineering reliability in that it provided a structured approach to modeling and analysis of how system failures could result in an undesirable consequence. As a result researchers were able to identify and assess alternatives to prevent catastrophic failures. It provided a tool from which to determine the general structure from which to perform a PRA analysis was outlined to involve [U.S. Reactor Safety Study, 1975]:

(1) identification of the sources of potential hazards,
(2) identification of the initiating events that lead to the potential hazards,
(3) identify all possible event sequences from which the potential hazards can originate,
(4) quantify each of these accident sequences through available data (frequency data) or best judgments, and
(5) determine the overall susceptibility to risk by calculating all event probabilities and their consequences.

Two modeling procedures using a "logic" tree form the basis from which to perform a PRA: the fault tree and the event tree. As observed in Figure 5.2, the fault tree addresses how a particular failure event could occur. The failure event is placed at the top of the tree and the intermediate causes of the failure event are identified and represented as a series of logical AND/OR gates that lead to that failure. The procedure is repeated until the final primary factors that initiate the potential failure sequences have been identified for each intermediate contributor.

The event tree, on the other hand, starts with an initiating fault or event and models each contributing factor in time to determine the sequence of factors that leads to an undesirable consequence. Figure 5.3 shows an event tree for the installation of an emergency shutdown valve in an oil pipeline [Bea and Moore, 1993]. The event tree distinguishes between decisions and events at various states of the system.

When PRA modeling was first developed, it was used solely for the purpose of modeling system failures and did not include the human element as an integral part of the failure analysis. After the nuclear power plant accident at Three Mile Island, it was apparent that the standard PRA did not sufficiently account for the reliability of the human operator at critical stages of the disaster. This inspired the development of the discipline of *human reliability analysis* (HRA), a discipline that integrates the human element into the PRA procedure. Swain and Guttmann (1983) define *human reliability* as "the probability that a person (1) correctly performs some system-required activity in a required time period (if time is a limiting factor) and (2) performs no extraneous activity that can degrade the system."

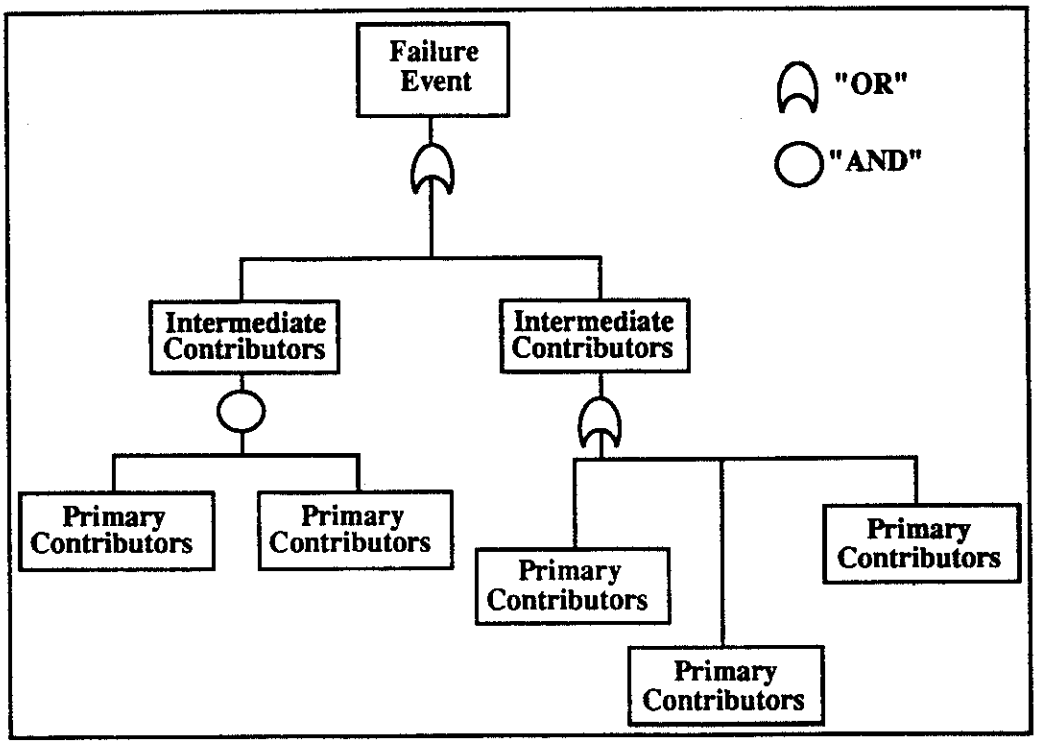


Figure 5.2 - Fault tree diagram

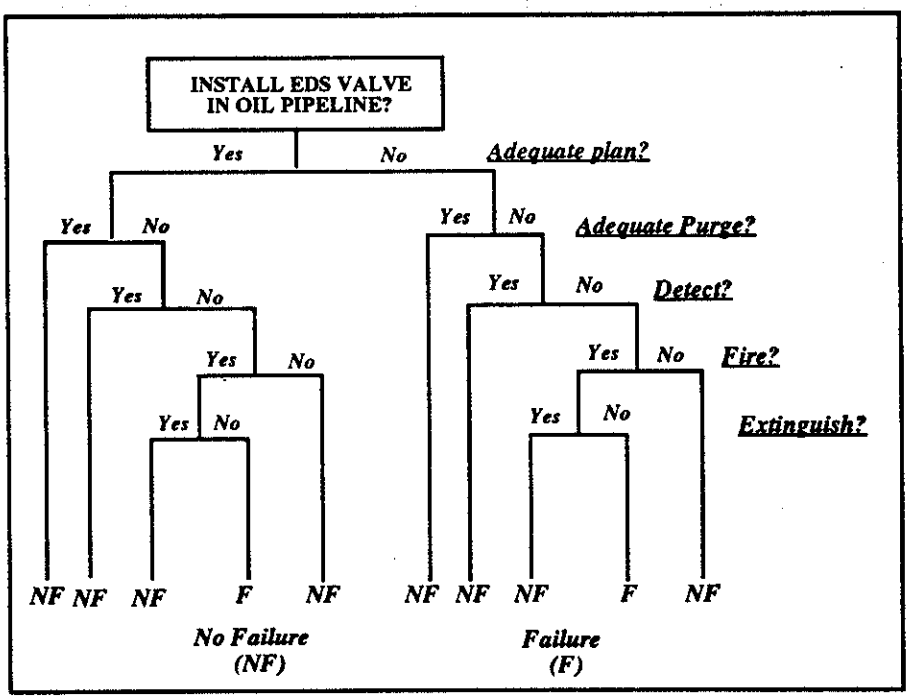


Figure 5.3 - Event tree for installation of ESD valve in oil pipeline [Bea and Moore, 1993]

5.2.1 Human Error Modeling Techniques

There have been a number of notable HRA techniques developed to quantify the human factor element in a formalized PRA analysis within the last two decades. The following is a short review of these techniques.

5.2.1.1 Technique for Human Error Rate Prediction (THERP)

The *Technique for Human Error Rate Prediction* (THERP) was introduced by Swain and Guttmann (1983) and has since become the most widely used human error prediction technique [Reason, 1990]. The THERP methodology were further developed and discussed in other publications related to human reliability for nuclear power plants [Bell and Swain, 1983; Swain and Weston, 1988; Haney, *et al.*, 1989]. The underlying theory of THERP focuses on modeling the human as any other sub-system in the PRA modeling process. This may be accomplished by a procedure similar to that described for the PRA analysis described above in Section 5.2. The steps are as follows [Swain and Guttmann, 1983]:

(1) identify all the systems in the operation that are influenced and affected by human operations,
(2) compile a list and analyze all human operations that affect the operations of the system by performing a detailed task analysis,
(3) determine the probabilities of human errors through error frequency data and expert judgments and experiences, and
(4) determine the effects of human errors by integrating the human error into the PRA modeling procedure.

Alternatives for prevention and mitigation (safety systems) could be integrated into the modeling procedure to determine their relative affects upon reducing the risks of human errors upon the system. Swain and Guttmann proposed that there are a set of *performance shaping factors* (PSFs) that influence the human errors at the operator level. These performance factors include experience, situational stress factors, work environment, individual motivation, and human-system interface. The PSFs are then used as a basis from which to estimate nominal values and value ranges for *human error probabilities* (HEPs).

One of the discrepancies of the fault or event tree analyses used is the reliance upon conditioning of error contributors that may not have a direct effect upon a human error at a particular stage in an accident scenario. Conditionalities between error factors and the errors are misdiagnosed and do not sufficiently model human errors or intervention to prevent the errors. THERP also neglected mistakes in addition to the selection of inappropriate strategies by operators to prevent or mitigate catastrophic events. These types of errors were particularly of interest in the Three Mile Island disaster. THERP was later revised to include modifications to accommodate their problems by focusing upon diagnostic errors and other levels of cognitive factors [Swain and Weston, 1988].

5.2.1.2 Confusion matrix technique

The confusion matrix technique is used to estimate the probabilities of initiating event misdiagnosis [Comer, *et al.*, 1984; Potash, *et al.*, 1981]. The focus is upon the actions that are performed to supplement the responses of technical system. The premise of the confusion matrix is to identify accident initiating events that are similar in appearance to the operators [Haney, *et al.*, 1989]. Each of the initiating events are listed on the horizontal and vertical axes of the matrix. Experiences and judgments of experts are used to rank which events would most likely be confused with the actual failure event by comparing how often they occur and how similar the symptoms are to the actual event. Probabilities

are then assigned to each misdiagnosis and the are modified to account for the operator training and abilities and control room layout and configuration.

Other matrices are constructed to model the misdiagnoses at different times in an accident sequence. The next step is to perform a frequency analysis for each "actual initiating event" and estimate the probability of misdiagnosis at each time in the accident sequence. The confusion matrix technique has been considered a good technique for qualitative assessments of potential failures in that it assists in identifying potential casualty causing contributors. However, the successes of the technique have been more qualitative than quantitative in nature. The confusion matrix is hampered by the same problems other HRA techniques are in its reliance upon expert judgments for probability based assessments.

5.2.1.3 Operator Action Tree (OAT)

The Operator Action Tree (OAT) method is used primarily as a tool for "estimating the likelihood of the operator's success in diagnosing the need for and ensuring the operation of necessary safety functions" [Henley, *et al.*, 1989]. The OAT procedure models the human's ability to react to an event through consideration of three stages: (1) observation of the event, (2) thinking about the event, and (3) responding to the event. The OAT procedure focuses primarily upon errors in diagnosis of problem and not errors in the response stages of an accident. Three primary steps are used to perform an OAT analysis [Henley, *et al.*, 1989]:

(1) Develop the parameters of an OAT by identifying safety functions from an event tree and then determine how the safety functions are achieved by system operation as shown in Figure 5.4. Identify the related human actions to perform the safety functions.
(2) Perform quantification of OAT by using analytical tool entitled the *time-reliability correlation* as shown in Figure 5.5.
(3) Transfer the identified operator's actions to the system fault or event trees in the formal PRA analysis procedure.

The time reliability correlation curve shown in Figure 5.4 is generated by both available data and expert judgment. The time available to the operators to make a problem diagnosis is called the thinking interval (T_t) and is defined as:

$$T_t = T_o - T_i - T_a \qquad (5.1)$$

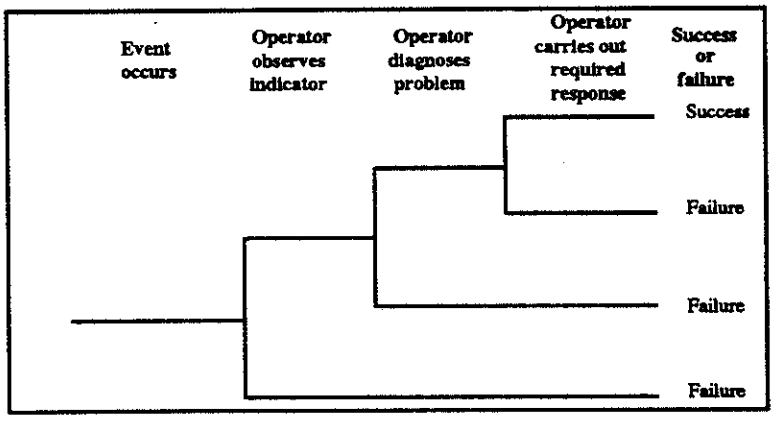


Figure 5.4 - Basic operator action tree [Henley, *et al.*, 1989]

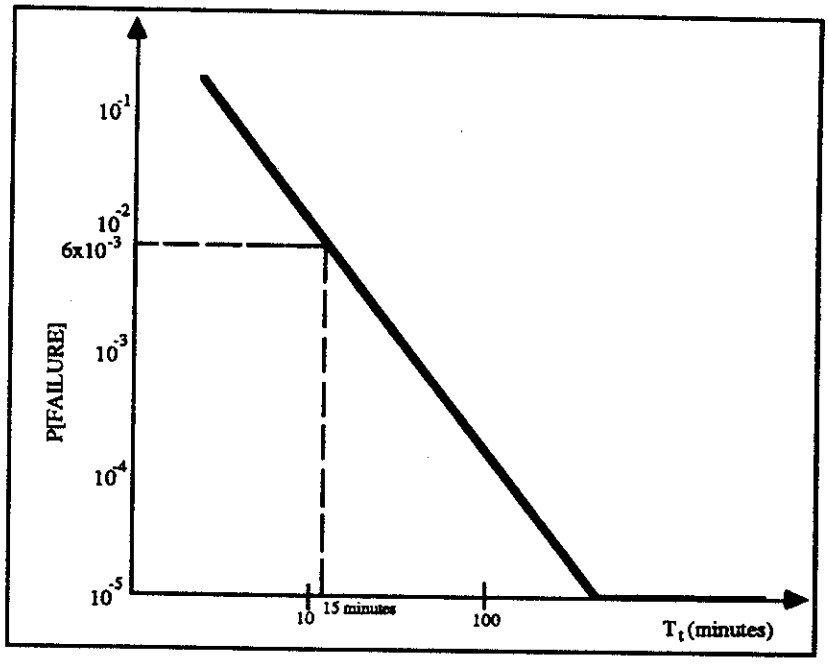


Figure 5.5 - Time-reliability correlation

where T_o is the overall time from the initiation of an accident sequence to the point by which actions need to be terminated, T_i is the time after initiation of a problem where indications of a problem are provided, and T_a is the time it takes to implement actions to alleviate the problem.

Attempts to verify these modeling procedures using simulator, historical and clinically based data judgment from 17 different sources related to different types of human actions met with limited success [Henley, *et al.*, 1989]. Further studies were performed that discussed the use of multiple human reliability curves based upon skill, rule, or knowledge based performances. These studies met with mixed success [Hall *et al.*, 1982]. However, sparse objective data has limited the capabilities of the OAT methodology due to its resultant reliance upon judgment or extrapolation from laboratory testing as its primary means for quantifying errors.

Each of the techniques described above has particular deficiencies in accounting for human errors as a result of organizational error factors. Human errors in many marine and non-marine related disasters have been shown to be directly influenced by ineffective management [Bea and Moore, 1993, 1994; Paté-Cornell, 1992; Royal Commission on the *Ocean Ranger* Marine Disaster, 1985]. None of the procedures explicitly address the impact of organizational behavior, culture, operations, or procedures upon human errors. Each of the techniques described above tend to focus on task related elements without trying to address norms and behaviors that are influenced beyond the limited scope of the direct interactions between the human and the system. Recent approaches to studying human reliability focus upon human errors affected by morale, organizational, and human related factors [Phillips, et. al, 1990]. These techniques form a basis for the human error modeling techniques developed in this report and are further discussed and described in Chapter 3 and Chapter 4.

5.3 PROBABILISTIC DEPENDENCE

Chapter 4 discussed establishing the "influence" (or *dependence*) between accident related events, decisions, actions, and errors created by human interaction with the operating system. The development of HOE template models to capture the general causative mechanisms of a particular accident scenario was described. The dependence between accident contributing factors may be *direct* or *indirect*. Direct dependence is defined as a factor directly affecting the outcome of factors to follow. Indirect dependence is the influence of factors which may change the influences between variables. Figure 5.6, shows the dependence of one particular random variable node (Y) upon a predecessor random variable node (X). One may describe this relationship by saying "X influences Y." The expression "Y|X" is stated as "the value of random variable Y given X has occurred."

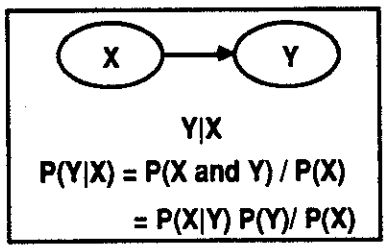


Figure 5.6 - General influence diagram representation of dependence

To demonstrate the relation of conditional and marginal probabilities variables, one uses *Bayes Rule*. If X_j and Y_i are mutually exclusive and collectively exhaustive events then Equations 5.2, 5.3, and 5.4 apply:

$$P[Y_i|X_j] = \frac{P[X_j \text{ and } Y_i]}{P[X_j]} \tag{5.2}$$

$$= \frac{P[X_j|Y_i]\,P[Y_i]}{P[X_j]} \tag{5.3}$$

$$= \frac{P[X_j|Y_i]\,P[Y_i]}{\sum_{i=1}^{n} P[X_j|Y_i]\,P[Y_i]} \tag{5.4}$$

where, $P[X_j] = \sum_{i=1}^{n} P[X_j|Y_i]\,P[Y_i]$.

5.3.1 Quantifying HOEs in Influence Diagrams

Human errors and contributors to human errors such as organizational errors, system complexities, human factors, and environmental factors, can be expressed either explicitly (solid arrows) or implicitly (dotted arrows) in an influence diagram. Explicit accounting of human errors and their contributors are represented by including a node for those factors within the influence diagram as shown below in Figure 5.7. One can implicitly account for human errors and their contributors by excluding them from the influence diagram. But the errors are accounted for by defining what effect errors will have on operational EDAs and casualty consequences and adjusting the quantitative measurement of the EDA accordingly. The nodes with dotted arrows represent factors that can be represented by an implicit influence. Examples of both explicit and implicit accounting of human errors in the influence diagrams are provided in Chapter 7.

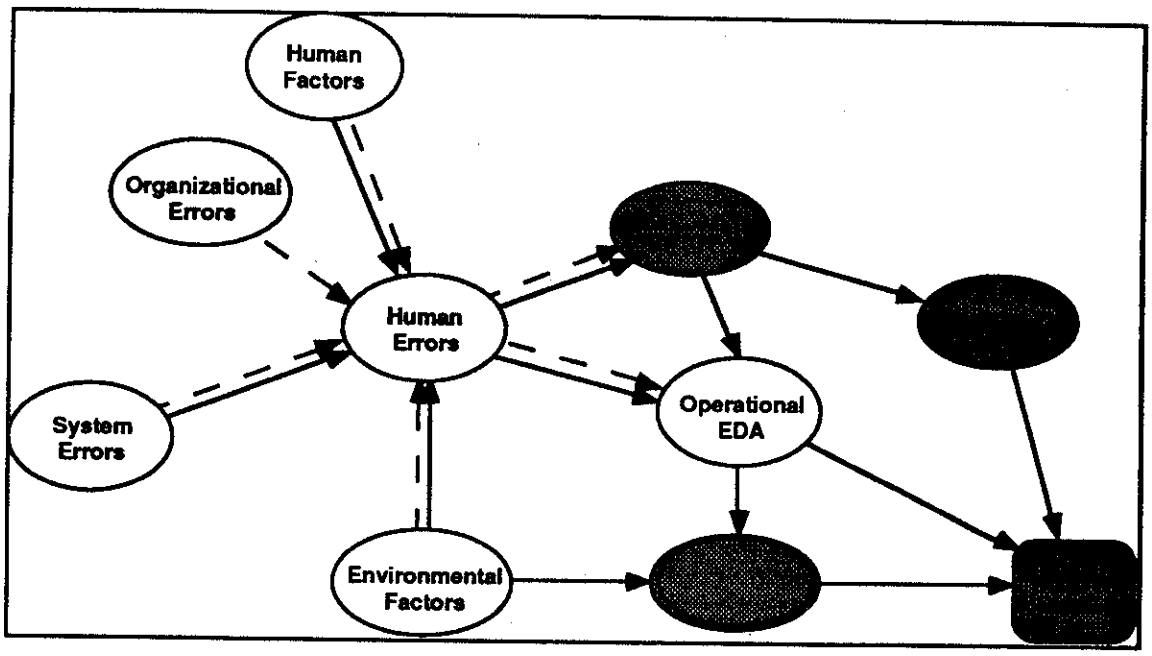


Figure 5.7 - Modeling human errors using influence diagrams

5.4 PROBABILITY ENCODING

Probability encoding allows managers, operators, engineers and regulators to use their experience and judgment (heuristics) to arrive at probability estimates for operational accident scenarios. Probability encoding entails the best guess of uncertain factors. In addition, probability encoding provides a means for communicating uncertainty in a decision analysis problem. In addition, it allows users to assess uncertainty based on intuitive assessment procedures related to their own limited judgments and experiences [Ashley, 1992; Spetzler and Staël von Holstein, 1972]. These differences can lead to bias in the quantitative modeling (biases are discussed in Section 5.4.2). This section discusses probability encoding and identifies associated biases and methods of identifying and mitigating bias in the encoding process.

5.4.1 Methods of Probability Encoding

The methods of probability encoding discussed in this section follow the work of Spetzler and Staël von Holstein (1972). Probability encoding may be either *probability* or *value* oriented. Probability methods ask questions on the probability of an identified value while keeping the value fixed. Value methods ask questions on a value scale while keeping the probabilities fixed. There also is the *probability-value method* in which probabilities and values are evaluated jointly.

The encoding process requires that responses be either *direct* or *indirect* through choices between simple bets. Direct response questions are those which require values for answers (e.g. "what is the probability of....?"). The responses are either given in probabilities, odds, values or fractions. On the other hand, indirect response questions are those in which you are asked to choose between alternatives (e.g. "would you prefer alternative A or B?"). Responses are choices between one alternative or another. The indirect method can then transfer the alternatives into probability assignments.

There are a number of probability encoding techniques which include using a "probability wheel", interval techniques, and assigning likelihoods to two well defined events.

However each method yield little information for low probability events. An inherent problem is that low probability - high consequence analyses are statistically vulnerable to low probability estimates [Freudenburg, 1988]. So probability encoding may be difficult to implement for these methods.

When using direct response modes, one may ask for a cumulative probability for a particular value (e.g. "what is the probability of an oil spill of 1,000 gallons or less?") or the probability of an event (e.g. "what size gas leak would correspond to a 5% probability?"). It has been observed that representing probabilities in a fractional method may be easier for the user to visualize. For example, "1 in 10" or "1 in 100" may be easier to conceptualize than ".1" or ".01." Expression in fractional terms are similar to odds and may be simpler to understand (particularly by those with non-technical backgrounds).

Estimates for using a direct response mode for the joint probability - value method may be used where the subject draws (or graphs) a density function, cumulative distribution, or a state of series of pairs of numbers (values with associated probabilities). This method is particularly useful for establishing probability distributions for magnitudes of particular events and may be described in the influence diagram procedure in a value node (see Section 4.2.2).

Verbal encoding uses verbal descriptors for particular events (e.g. "low", "medium", or "high" gas production rates used in Section 7.3 for *Piper Alpha* disaster example). This method produces relative magnitudes of particular contributors without having to make discrete value assessments. Verbal encoding is useful for inputs with relative or no particular value yet probabilistic assessments are necessary.

5.4.2 Biases in Probability Encoding

It may (or may not) be simple to arrive at a probability for uncertain values. But, biases usually are incorporated into the probability assessments. This section identifies the sources and types of biases which may affect the probability encoding process. Bias may be *motivational* and *cognitive* in nature and are described by Spetzler and Staël von Holstein (1972) as:

Motivational bias:
"either conscience or sub-conscience adjustments in the subject's responses motivated by his perceived system of personal rewards for various responses..."

Cognitive bias:
"either conscience or sub-conscience adjustments in the subject's response systematically introduced by the way the subject is intellectually processing this perceptions..."

Motivational bias is of concern if the subject has a vested interest in the of the model outcome. Subjects may present either overly optimistic or pessimistic probability assessments dependent upon whether the outcome has a direct effect upon their well-being. For example, an offshore production manager may state lower production levels to management in order to exceed those production levels (paralleling organizational and human incentive errors). Cognitive bias is related to the subject's abilities to grasp the details and inter-relationships of variables and issues within the problem. As discussed in Section 3.2.1 and 3.2.2, a cognizance of contributing factors (human and system) is essential to the modeling process.

Bias arises as a result of what are called *modes of judgment.* Modes of judgment are the basis from which the subject generates his or her probability estimates. It is important for those preparing the user (i.e. the interviewer) to determine the modes of judgment being used by the subjects in order to avoid excessive probabilistic biases. If the encoding process is performed correctly, the described biases are minimized. The modes of judgment are:

(1) *Availability*: Probabilistic assignments are based upon the information subjects may recall or visualize. The probabilities of events are assessed from the recollection of the subject to events of the same nature. For example, an engineer may be asked to provide a probability assessment for the failure of a condensate pump. The engineer would give an assessment based upon the failure of similarly designed pumps in his experience. Care should be taken in using subject availability since recent information is often given too much weight and other relevant information is not properly incorporated into the analysis.

(2) *Adjustments and anchoring*: Available information often forms a basis from which subsequent responses represent adjustments from that basis. For example, the most current of information is thought to carry the most weight with little regard to longer trends. Anchoring results in a centralized bias. As shown in Figure 5.8, central bias (distribution B) is where a distribution is smaller than what is justified for a particular uncertainty in a variable. Anchoring can be the outcome of certain information being available at the initiation of the modeling procedure and other relevant information being suppressed. It is the result of a failure to address other points under consideration independently from the central point.

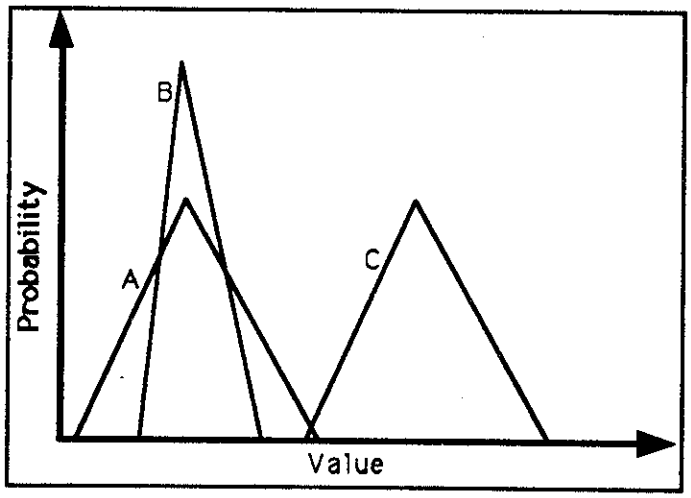


Figure 5.8 - Descriptive diagram of variability and displacement biases

(3) *Representativeness*: Probability assessments or judgments which are similar in distribution or nature to other probability assessments. These distributions assignments may be of use to one industry but not for another. For example, stress levels for front-line operators of nuclear power plants may be estimated by those of front-line operators of oil refineries. Stress levels may be considerably higher at nuclear power plants as a result of the catastrophic consequences of potential accidents. Though the operations may be similar, other contribut-

ing factors should be taken into consideration to arrive at probability assessments. Representative bias can be reduced by further structuring the problem to account for additional variables that distinguish one operation from another.

(4) *Unstated assumptions*: Probability assessments are most often conditional upon a number of unstated assumptions. This leads to a lack of consideration of important contributing factors. Model assumptions should be communicated in advance of the modeling procedure.

(5) *Coherence*: Probability assignments are based upon the ease in which a scenario is fabricated. Other scenarios which may lead to catastrophic events are disregarded or viewed as too remote (see Section 4.3.1).

5.4.3 Encoding Interview Process

An advantage of probability encoding is that it allows a broad range of subjects to observe the problem with the same set of conditions. For example, engineers and managers may view odds in two different ways; one views rolling the dice (the manager) while another visualizes an integral equation (the engineer). One goal of the encoding interview process is to ensure all subjects are "on the same page." In other words, it is vital that engineers, regulators, operators, and managers have a similar understanding of the probabilistic measuring process regardless of how the information is being processed by the individual. Of course there are differences in probability assignments between individuals as a result of their experiences and judgments.

There are five general steps to the encoding process as described by Spetzler and Staël von Holstein (1972) and are described in the following sections.

5.4.3.1 Motivating

Developing a rapport with the experts involved in the modeling and decision process to identify any possible motivational biases. The goals of this phase are to introduce the experts to the encoding tasks and the differences between deterministic and probabilistic predictions of variables (see Section 4.2.2.1). In addition, this step allows the interviewer an opportunity to explore for motivational biases of the experts (subjects).

5.4.3.2 Structuring

This step is important to identify uncertain quantities to be defined in the model. This step entails clearly communicating the model variables. The experts should be able to pass what is called the *clairvoyance test*: a clairvoyant should be able to specify the outcome of variables without asking additional questions. For example, if "vessel traffic" is a variable, it does not specify the location, time of day, etc. However, if the variable was identified as vessel traffic in the Valdez Narrows of Prince William Sound, then the information is much clearer in its interpretation such that the expert need not require additional information to make a valid estimate.

5.4.3.3 Conditioning

Conditioning is necessary in the development of fundamental judgments and avoidance of cognitive biases. The primary goals is to communicate with the expert group to ensure all members are using the same group of assumptions and are perceiving the problem in the same structured way. This step is the important in identifying bias. Here the experts are asked to identify the sources of the values they have assigned to each of the variables. For example, if an expert identifies a realistic high consequence (e.g. 10 people injured) for a particular accident event, the interviewer would ask if from what source is the judgment being derived? Does it parallel a recent similar accidents?

5.4.3.4 Encoding

The encoding step is the direct quantification of heuristic judgments in terms of probability assignments. Distinction are made between direct human related factors (HOEs, decisions, and actions) and events or consequences. Human related factors are dependent upon the error classifications described in Chapter 3. A general method for encoding these factors is described below.

Probabilistic encoding of events and consequences are assessed to arrive at cumulative distributions for magnitudes of accident events. One may estimate events and consequences by the following method:

(1) Ask for extreme value event (least and worst case scenarios) assignments of casualty consequences provides a set of boundaries in which the probability modeling will occur (see Figure 5.9). Generally, the larger the spread, the greater the uncertainty.

(2) Ask for the probability or odds of the extreme values. Elicit some scenarios that may assist in the value assignments.

(3) Explore values between the extreme values by using the *interval technique*. The interval technique entails splitting an interval into two sections and asking which part the expert agrees is most likely. The dividing point is changed until the subject is indifferent between the intervals. This point is recorded as the median value. The intervals are further sub-divided and the process repeated. The quartile values are obtained and recorded. The intervals may be further subdivided and the method repeated but may be subjected to compounding errors from the median and quartile estimates. Therefore, further subdivision should be used with caution.

    The extreme, median, and quartile values are recorded on probability paper using either probability or cumulative probability distributions for this report cumulative distributions are used. Figure 5.9 is a description of the points chosen. A curve fit may be drawn (or generated on a computer) for the points as shown in Figure 5.10.

(4) One may wish to derive discrete probability assessments from the curve fit shown in Figure 5.10. Given a continuous probability distribution, the distribution is distinguished into probability intervals shown in Figure 5.11. The number and sizes of the intervals are at the discretion of the user. Horizontal lines are drawn crossing through the curve. The break points for the values are at A, B, and C. Within the interval [0,A] a vertical line is moved until the shaded areas are equivalent in size. The value associated with the equivalent areas, A, is recorded as the value associated with probability p_1. The process is repeated for intervals [A,B] and [B,C]. The final outcome is equivalent to the discrete probability distribution shown in Figure 5.12. The probabilities and associated values are input into the variables of the influence diagram model.

5.4.3.5 Verification

Verifying is checking the responses in the probability encoding to ensure consistency. The judgments of the experts are checked to see if they truly believe in them. There are two parts to the verification procedure. First, the cumulative distributions generated by the encoding process are used as a means of feedback to determine if the distribution is consistent with their judgments. This verification method is important for examining

probabilities in the extreme values ranges (see Figure 5.10; value intervals $[0,v_1]$ and $[v_5, \infty)$). Second, is to choose a sequence of value pairs to determine if the values would be equally attractive. This is accomplished by using the method described in the preceding section for determining median and quartile values. Additional values are chosen lying between the median and quartile intervals to determine if the curve is consistent with experience and judgment. This process should be performed 3 to 5 times to acquire confidence in the curve.

5.4.4 Sensitivity Analysis

Sensitivity analysis is used to measure the importance of a decision or state variable included within the influence diagram model. Decision variables may or may not be part of the QRA modeling procedure. However if decision variables are included, the procedure below is used to determine the impact of the decision upon the model.

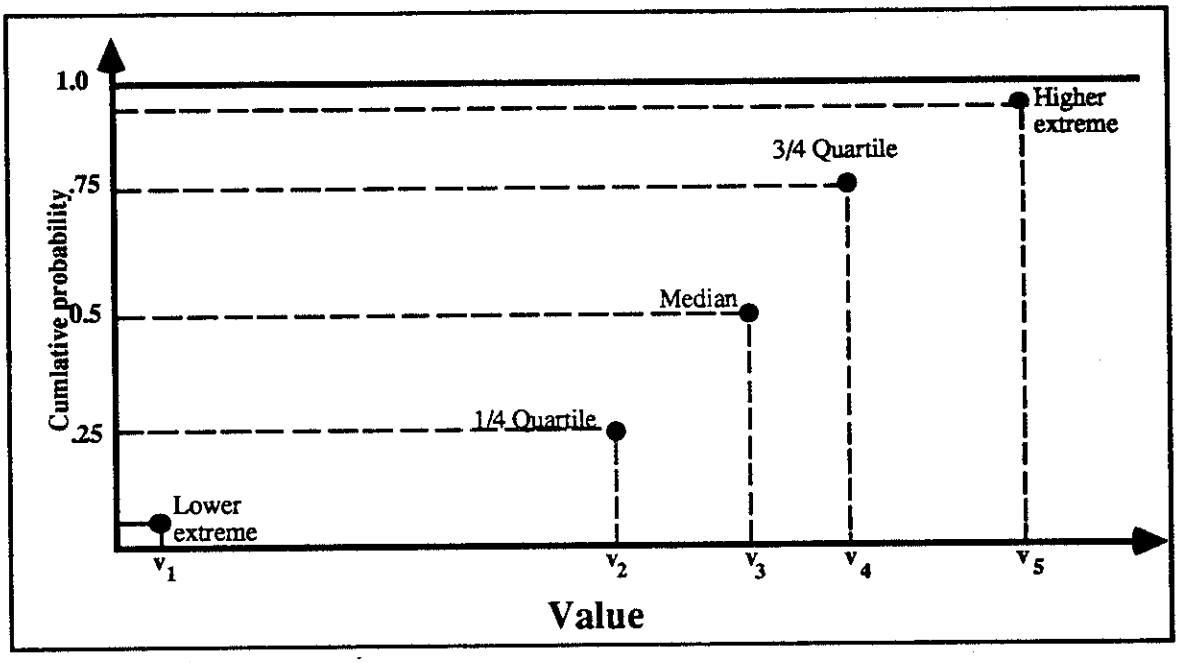


Figure 5.9 - Distribution of points for probability encoding

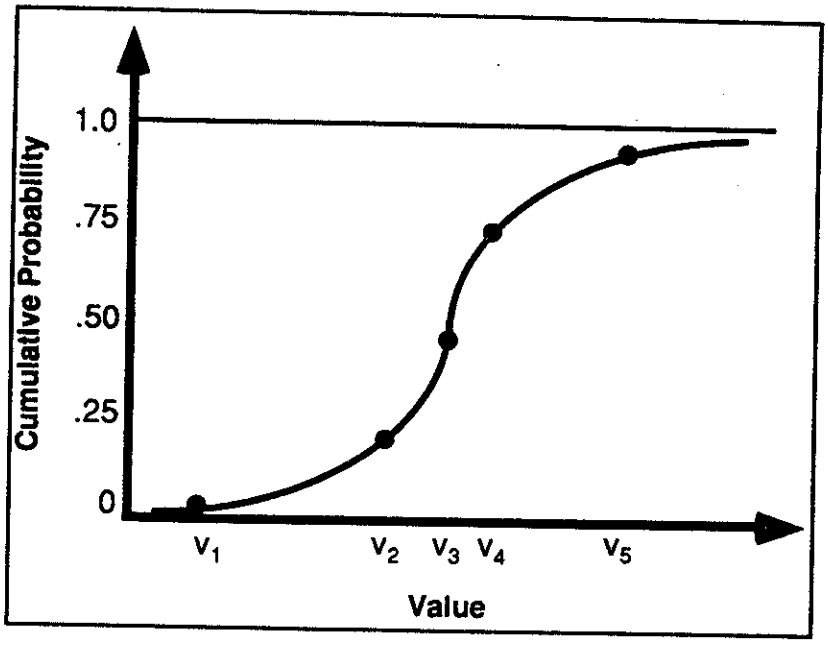


Figure 5.10 - Curve fit of point distribution for probability encoding

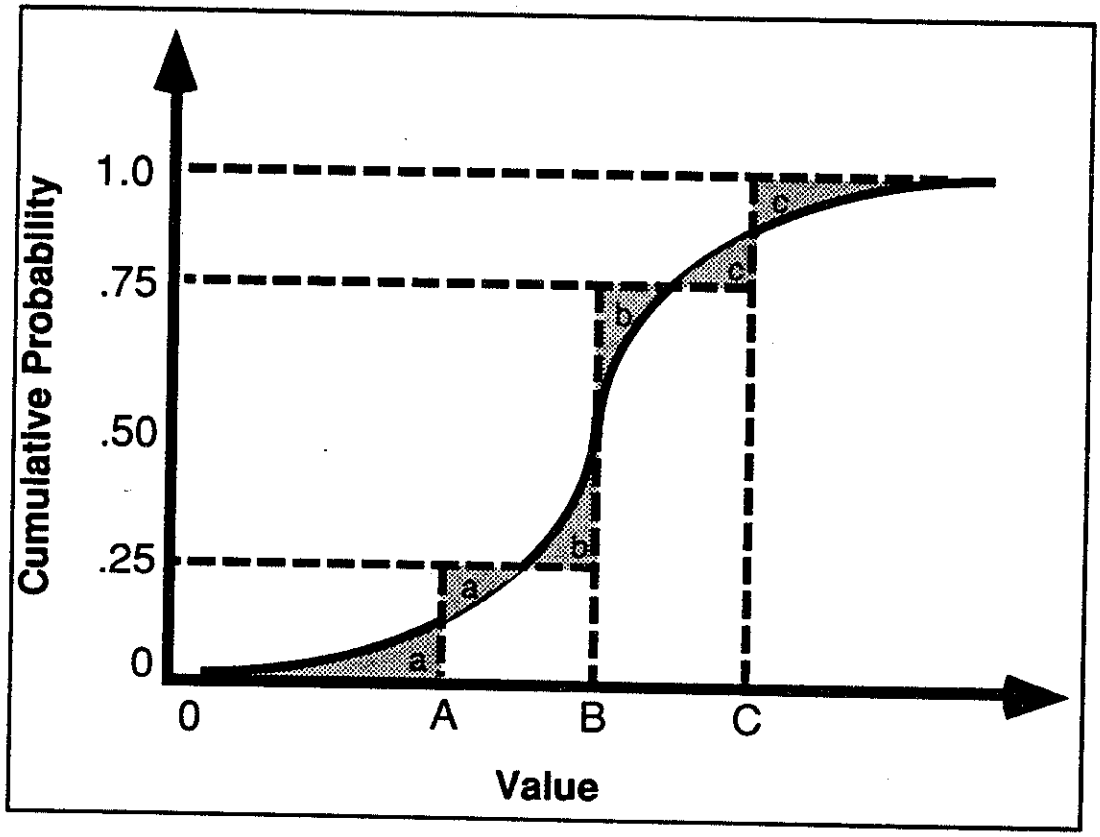


Figure 5.11 - Discretization of probability distributions

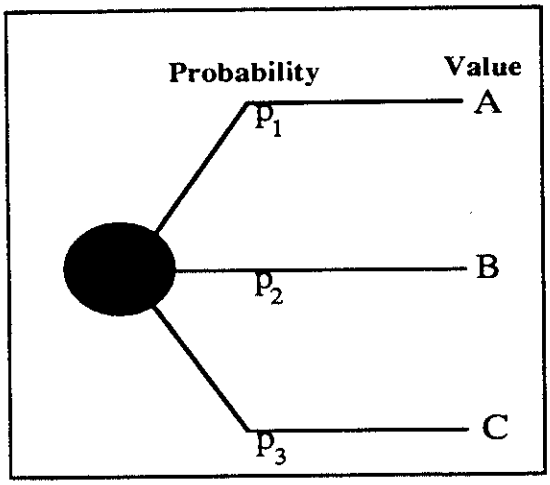


Figure 5.12 - Discrete probability distribution equivalent for discretization process

In Chapter 4, we discussed the development of influence diagram templates. In the process of developing an accident framework model, it is important to perform sensitivity analysis on contributing variables to determine their importance to the model. The advantages of this are twofold. First, they allow the user to determine the impact of decision and state variables upon a model in an effort to formulate the influence diagram template. Second, the template has been developed as a basis from which to model unique operating conditions at different times, locations, or operating procedures. Additional decision or state variables unique to the operating system may need to be included. This section discusses the sensitivity analysis procedure.

Sensitivity analysis are performed on both decision and state variables. The following procedure describes the methods used for sensitivity analysis on decision variables and state variables.

(1) After developing the influence diagram model representation (Sections 4.3 and 4.4) the influence diagram and remove all variables which may be eliminated through heuristic judgment.

(2) Fix all the nominal values for state variables (probability variables) in the model. The nominal values may be obtained through the probability encoding procedure methods described above, the HESIM, casualty data, or other sources.

Decision Variables (when applicable):

(3a) Determine the sensitivity of the final outcome to the variability in decisions. This is accomplished by using the influence diagram program *InDia* and is further described in Appendix 4.

(4a) Retain the decisions whose variability has substantial impact upon the outcome of the model. Delete the decisions from the model which have only small effects on the overall outcome.

State Variables:

(3b) Determine the sensitivity of the final outcome to the range of possible values in state variable similar to (3a).

(4b) Retain the state variables whose variability has substantial impact upon the outcome of the model. For state variables, it is not necessary to delete the variable from the model if the impact is negligible. The variable may be made deterministic by leaving it at the original nominal value chosen.

This simple procedure assists the user in determining the importance of the variables of the models being included. Examples of this procedure are used for the cases studies described in Chapter 7.

5.5 HUMAN ERROR SAFETY INDEX METHOD (HESIM)

Gale (1993) describes safety (or risk) index methods as a modified quantitative risk assessment procedure in which key risk contributors are identified, assessed and assigned numerically weighed values. In the absence of probabilistic data identifying contributions of HOEs in marine casualties, developing quantitative safety indices allow for examination of relative risks to operational safety. Comparisons are drawn between safety indices and human error frequencies leading to greater certainty in risk index measures.

5.5.1 Background of Risk Indices in Industrial Measuring Safety

Safety index methods have been used in a number of industries to determine relative safety. Bello and Colombari (1980) developed a human error risk index method entitled *technica empirica stima errori operatori* (TESEO) using interview data collected from petrochemical plants. The TESEO method is used to arrive at the probability of failure using 5 general operator parameters: (1) type of activity, (2) temporary stress factors for routine activities, (3) operator qualities, (4) an activity anxiety factor, and (5) an activity ergonomic factor. Fire and explosion risk indices have been created for refineries, offshore platforms, hospitals, and chemical processing plants [American Institute of Chemical Engineers, 1987; Gale, 1993; Imperial Chemical Industries, 1980; Nelson and Shibe, 1978]. In addition, index methods have been used for offshore platform structural requalification and pipeline assessments [Bea and Craig, 1993; Mulhbauer, 1992].

The safety index method described in this report is called the *Human Error Safety Index Method* (HESIM). In Chapter 3, the error classification had been proposed to categorize human, organizational, and system errors leading to human errors at the operational level. The HESIM integrates error inducing parameters (error solicitors) that can lead to an accident event. The error solicitors are organizational, human, task, system, and environmental factors.

5.5.2 Contributing Factors to the HESIM

The HESIM incorporates error factors from four primary contributors: (1) organizational, (2) human, (3) system, and (4) the operating environment. Table 5.1 shows a further categorization of the primary contributors (see Sections 5.5.2.1 through 5.5.2.4).

5.5.2.1 Organizational factors

Figure 5.13 demonstrates the contribution of organizational errors at various levels which may lead to a human error at the operator level. A potential HOE solicitor (event, decision, action, environmental operating condition, etc.) affects the front-line operation. However, the error may be the result of underlying organizational factors. These factors are relatively static over short periods of time in a single operating environment (vessel or platform). The potential error solicitor "filters through" the "static" safety management system at the organizational level. If the management system is reliable, the effect on front-line operators can be reduced. However, if the management system does not respond sufficiently to handle a potential error solicitor, front-line operator errors may increase.

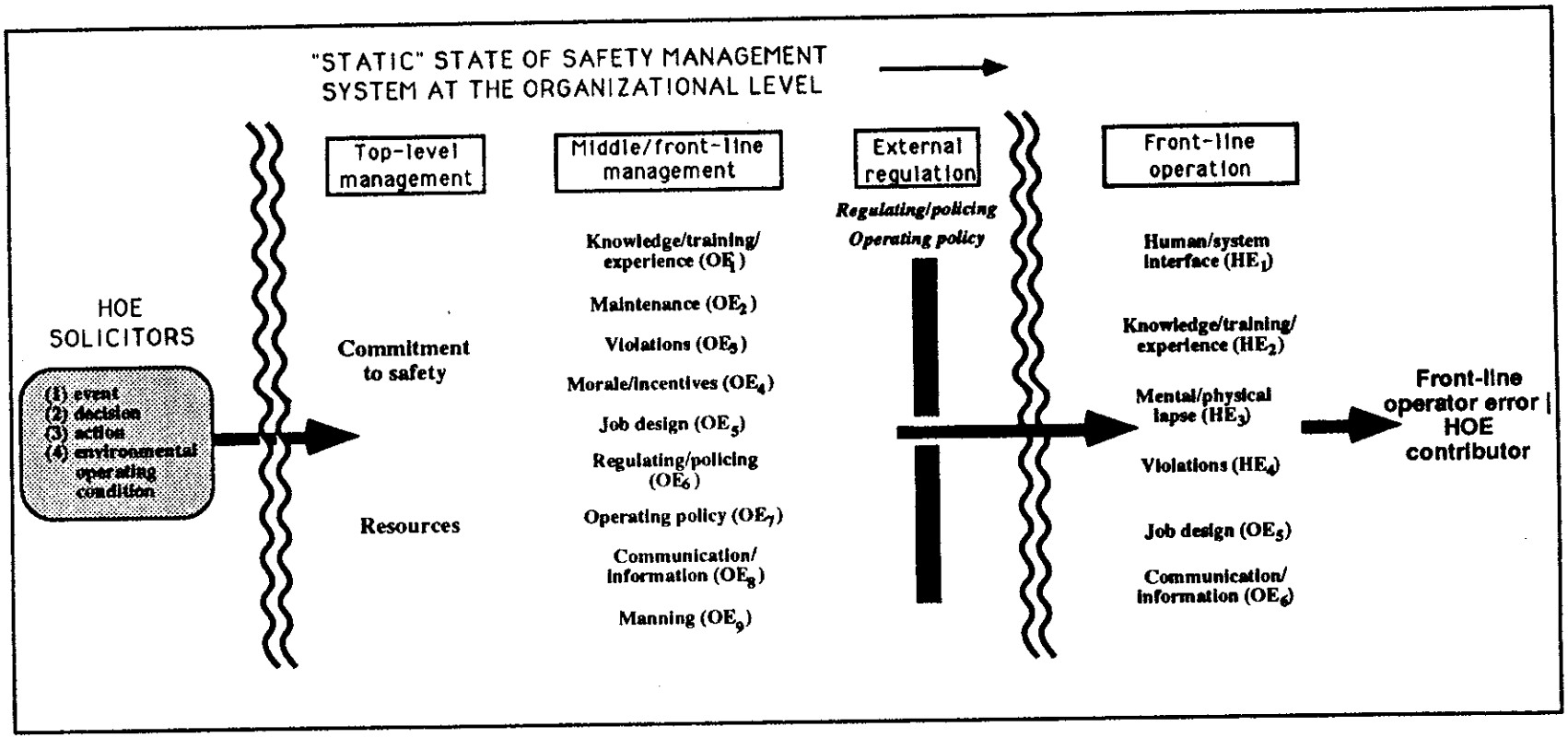


Figure5.13: Human, organizational, and regulatory impacts on human errors at the front-line operator level

Table 5.1 - Categorization of contributing factors to the Human Error Safety Index Method

ORGANIZATION	HUMAN	SYSTEM	OPERATING ENVIRONMENT
Top-level Management	Stress	Complexity	External
Middle - Front-line Management	Routineness		Internal
Regulatory			

Organizational contributing factors are categorized into *top-level management* (TLM) and *middle or front-line management.* Top-level management is responsible for development of organizational strategies and company goals. It is primarily the responsibility of middle and front-line managers to provide a means by which TLM goals are realized. Therefore, TLM error contributors are categorized as *commitments to safety* and *resources*. As discussed in Chapter 3, a commitment to safety begins at top-level management to ensure commitments to safety at the operator level (see Chapter 3: *source failure types).*

Commitments to safety and resources allocated at TLM filter down into the middle and front-line operations and affect organizational errors that may directly or indirectly affect errors at the operator level (see Chapter 3: function failure types). These errors are either reduced or compounded as they are tested by external regulation. External regulation is categorized into *regulating and policing* and *operating policy*. The operating policy establishes the boundaries in which the organizations may operate. Operating policy is most effective if implemented in conjunction with regulating and policing. If regulating and policing are effective, safety is enhanced since operators are held responsible and accountable for their actions and can, in effect, lead to a reduction of management errors.

5.5.2.2 Human factors related to error initiator

Two human related factors result from HOE solicitors: *stress* and *routineness*. Errors can be categorized by errors of *omission* and errors of *commission* [Reason, 1990; Swain and Guttmann, 1983]. These errors are directly related to operator tasks being performed. Errors of omission are defined as errors in which critical tasks are not performed. Errors of commission are errors in which tasks are incorrectly performed. Both types of errors can be the result of human factors related to the initiating factor.

5.5.2.2.1 Operator stress

Figure 5.14 is a descriptive diagram of human performance under various levels of operating conditions. Operator errors are magnified and compounded in times of stress or panic [Heising and Grenzebach, 1989; Offshore Certification Bureau, 1988; Panel on Human Error in Merchant Marine Safety, 1976; Swain and Guttmann, 1983; Wenk, 1986]. Optimal performance levels are observed at an "appropriate level of arousal" [Melchers, 1976]. Human performance levels vary between individuals depending upon training, variability among individuals, organizational pressures, and complexity of the operating system. Nevertheless, performance is observed to deteriorate when pressure levels are either too low or too high. For example, high pressures could effect stress or panic, and low human performances could be the result of boredom or laziness. Both extremes can contribute to incidence of human error.

Stress level is assumed independent of the complexity of the operating system. For instance, if operator knowledge, training, or experience is adequate for operation of the task, the complexity of the operating system and the routineness of the tasks performed might not be affected. Therefore, operator stress, system complexity, and task routine are measured independently.

5.5.2.2.2 Routineness

Routineness measures the simplicity or complexity of the tasks being performed. The greater the routineness the greater the familiarity with the tasks leading to a higher level of safety. When the tasks are complex there is a greater risk of errors associated with that task.

5.5.2.3 Operating system complexity

The complexity of the operating system is related to the effectiveness in which information is provided by the system. It is assumed that the greater the system complexity, the higher the chance of errors occurring independent of the routine nature of the EDA. In Chapter 3, system errors are classified into *communication* and *information* and *human system interface*. The question at hand is: "Does the system provide sufficient information and communicate it in a fashion to allow for a correct and timely course of decision and action?"

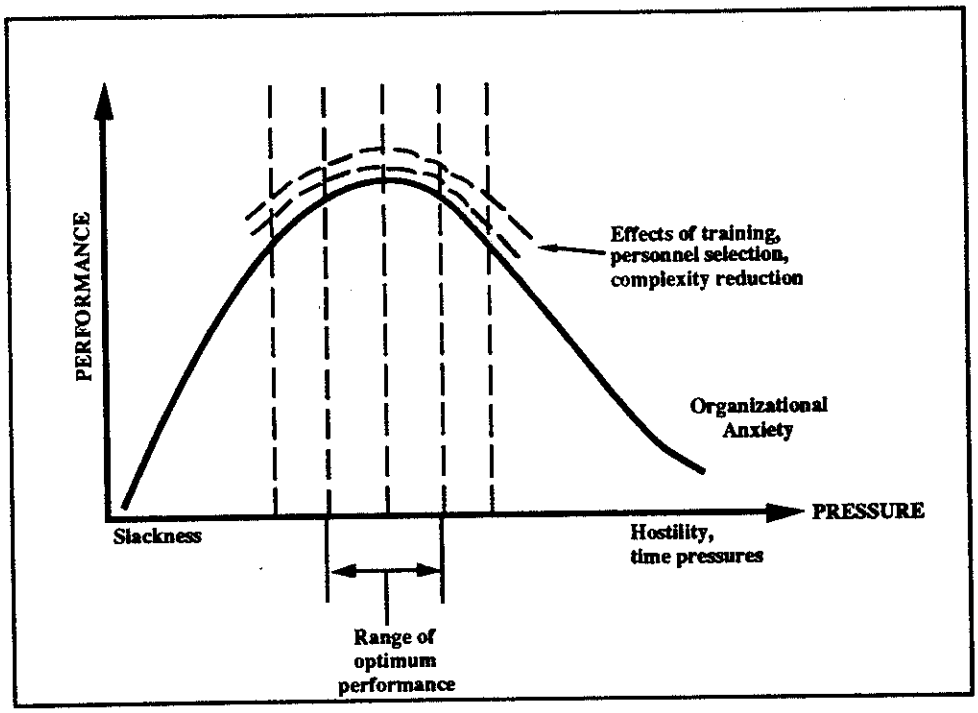


Figure 5.14 - Human performance function [Melchers, 1987]

5.5.2.4 Operating environment

As mentioned in Chapter 3, environmental operating conditions can contribute to accident scenarios. Environmental conditions are categorized into *external* or *operational* conditions (see Table 3.1).

5.6 THE *HUMAN ERROR SAFETY INDEX ALGORITHM*

The HESIM is a consolidation of heuristic approaches and the development of an accident database. As detailed accident data becomes more available for particular accident classes, the risk indices are refined to correlate with the casualty statistics. This section describes the HESIM algorithm which integrates the contributing factors described in the previous section. Chapter 3 provides a set of initial heuristic HESIM measures used for case study examples described in Chapter 7. The conditional human error index is used as a quantitative measurement for the influence diagram modeling. It is not a probabilistic measure, but a means by which to systematically quantify human errors. These measures form a basis from which future error index refinements, modifications, and verifications are made until sufficient data is available to use probabilistic measurements.

Equation 5.5 is the generalized equation integrating contributing casualty factors defined in Section 5.5.2. The overall human error index is the quantitative measurement of human and organizational errors, human factor, system, and environmental factors occurring for a specified event, decision, or action. The *overall human error safety index* ($SI_{HEi,OEj,HF,Env,Syst,EDAq}$) is the product of five safety indices: (1) the *human error safety index* ($SI_{HEi|OEj,HF,Env,Syst,EDAq}$) (2) the *organizational error index* ($SI_{OEj,EDAq}$), (3) the *human factor index* ($SI_{HF,EDAq}$), (4) the *system index* ($SI_{Syst,EDAq}$), and (5) the *environmental index* ($SI_{Env,EDAq}$).

$$SI_{HE_i,OE_j,HF,Syst,Env,EDA_q} = k_{ij} SI_{HE_i|OE_j,HF,Syst,Env,EDA_q} * SI_{OE_j,EDA_q} * SI_{HF,EDA_q} * SI_{Syst,EDA_q} * SI_{Env,EDA_q} \quad (5.5)$$

Each safety index SI, lies between 0 and 1 and k_{ij} is a factoring constant for human error i and organizational error j.

$$0 \le SI \le 1$$

As shown in Equation 5.6, the measure of the overall human error safety index is a weighted frequency of the factors for a specified class of accidents (e.g. tanker collisions or grounding, offshore production-maintenance explosions, and fires). Weighted values are assigned depend upon the certainty of that factor being a contributor to a casualty-near miss sequence. The error frequency is determined by averaging across the weighted frequencies of joint occurrences between MOEs and HEs under all external operating conditions, human factors, and system complexity. The information is input into the appropriate cell of the data HOEDQS described in Section 5.7 and Chapter 3. For each casualty-near miss, the associated human, organizational, human factor, system, and environmental contributor is documented. The certainty values are placed in the proper location for the joint occurrences as shown in Table 5.2.

$$\left\{SI_{HE_i,OE_j,EDA_q,HF,Syst,Env}\right\}_k = 1 - \left\{f_{HE_i,OE_j,EDA_q,HF,Syst,Env}\right\}_k = 1 - \frac{1}{m}\sum_m \left\{\xi_{HE_i,OE_j,EDA_q,HF,Syst,Env}\right\}_{km} \quad (5.6)$$

Table 5.3: Safety indices of human associated organizational errors for accident class n with consequence v_k and event, decision, or action q

Human Errors (HE_i)	know/ training/ exper (MOE_1)	maint-enance (MOE_2)	violation (MOE_3)	morale/ incentive (MOE_4)	job design (MOE_5)	regul/ policing (MOE_6)	operating policy (MOE_7)	comm/ info (MOE_8)	manning (MOE_9)	none (MOE_{10})	
Top level management (TLM)	x $SI_{MOE_1/TLM}$	x $SI_{MOE_2/TLM}$	x $SI_{MOE_3/TLM}$	x $SI_{MOE_4/TLM}$	x $SI_{MOE_5/TLM}$	x $SI_{MOE_6/TLM}$	x $SI_{MOE_7/TLM}$	x $SI_{MOE_8/TLM}$	x $SI_{MOE_9/TLM}$	x $SI_{MOE_{10}/TLM}$	*Marginal Safety Index of HE_i* (SI_{HE_i})
hum/syst interface (HE_1)	$SI_{HE_1OE_1}$	$SI_{HE_1OE_2}$	$SI_{HE_1OE_3}$	$SI_{HE_1OE_4}$	$SI_{HE_1OE_5}$	$SI_{HE_1OE_6}$	$SI_{HE_1OE_7}$	$SI_{HE_1OE_8}$	$SI_{HE_1OE_9}$	$SI_{HE_1OE_{10}}$	$\{SI_{HE_1}\}_k = \sum_j \{SI_{HE_1OE_j}\}_k$
know/train/ exper (HE_2)	$SI_{HE_2OE_1}$	$SI_{HE_2OE_2}$	$SI_{HE_2OE_3}$	$SI_{HE_2OE_4}$	$SI_{HE_2OE_5}$	$SI_{HE_2OE_6}$	$SI_{HE_2OE_7}$	$SI_{HE_2OE_8}$	$SI_{HE_2OE_9}$	$SI_{HE_2OE_{10}}$	$\{SI_{HE_2}\}_k = \sum_j \{SI_{HE_2OE_j}\}_k$
mntl/phys lapse (HE_3)	$SI_{HE_3OE_1}$	$SI_{HE_3OE_2}$	$SI_{HE_3OE_3}$	$SI_{HE_3OE_4}$	$SI_{HE_3OE_5}$	$SI_{HE_3OE_6}$	$SI_{HE_3OE_7}$	$SI_{HE_3OE_8}$	$SI_{HE_3OE_9}$	$SI_{HE_3OE_{10}}$	$\{SI_{HE_3}\}_k = \sum_j \{SI_{HE_3OE_j}\}_k$
violations (HE_4)	$SI_{HE_4OE_1}$	$SI_{HE_4OE_2}$	$SI_{HE_4OE_3}$	$SI_{HE_4OE_4}$	$SI_{HE_4OE_5}$	$SI_{HE_4OE_6}$	$SI_{HE_4OE_7}$	$SI_{HE_4OE_8}$	$SI_{HE_4OE_9}$	$SI_{HE_4OE_{10}}$	$\{SI_{HE_4}\}_k = \sum_j \{SI_{HE_4OE_j}\}_k$
job design (HE_5)	$SI_{HE_5OE_1}$	$SI_{HE_5OE_2}$	$SI_{HE_5OE_3}$	$SI_{HE_5OE_4}$	$SI_{HE_5OE_5}$	$SI_{HE_5OE_6}$	$SI_{HE_5OE_7}$	$SI_{HE_5OE_8}$	$SI_{HE_5OE_9}$	$SI_{HE_5OE_{10}}$	$\{SI_{HE_5}\}_k = \sum_j \{SI_{HE_5OE_j}\}_k$
comm/info (HE_6)	$SI_{HE_6OE_1}$	$SI_{HE_6OE_2}$	$SI_{HE_6OE_3}$	$SI_{HE_6OE_4}$	$SI_{HE_6OE_5}$	$SI_{HE_6OE_6}$	$SI_{HE_6OE_7}$	$SI_{HE_6OE_8}$	$SI_{HE_6OE_9}$	$SI_{HE_6OE_{10}}$	$\{SI_{HE_6}\}_k = \sum_j \{SI_{HE_6OE_j}\}_k$

$$\xi_{\substack{HE_i, MOE_j EDA_q, TLM \\ HF, Syst, Env}} = \begin{cases} 0 \text{ no relation} \\ \frac{1}{3} \text{ "low" certainty of relation between } HE_i \text{ and } MOE_j \\ \frac{1}{2} \text{ "moderate" certainty of relation between } HE_i \text{ and } MOE_j \\ 1 \text{ "high" certainty of relation between } HE_i \text{ and } MOE_j \end{cases}$$

where k is the consequence level of the casualty, and m is the total number of operations per measurement of time for that consequence level.

The human error index is the quantitative measurement of human error conditional upon a set of organizational errors, human factors, system and environmental factors for a specified EDA. By solving for the human error index of Equation 5.5 to arrive at Equation 5.7, one is able to use these values as quantitative measurements of human errors under varying organizational, human factor, system, and environmental conditions. Again it should be noted that the human error index generated by this technique is not a probability, but an index value conditional upon any number of error solicitors. These are the conditional safety indices that are used in the influence diagram model quantitative procedures described above in Section 5.4.1.

$$\left\{SI_{HE_i|OE_j, HF, Syst, Environ, EDA_q}\right\}_k = \frac{\left\{SI_{HE_i, OE_j, HF, Syst, Environ, EDA_q}\right\}_k}{k_{ij} * SI_{OE_i, EDA_q} * SI_{HF, EDA_q} * SI_{Syst, EDA_q} * SI_{Env, EDA_q}} \quad (5.7)$$

The next step is to provide a methodology for measuring the safety indices in the denominator of Equation 5.7. The *organizational error safety index* ($SI_{OEj,EDAq}$) shown in Equation 5.8 is a measure of the impact of top-level management upon mid-level management and operator level management errors (MOE) effects upon human errors (HE) at the operator level. A matrix representation of Equation 5.8 is shown in Table 5.3. The index is assumed to be relatively static over short periods of time for any given operation [Reason, 1992].

$$SI_{OE_j, EDA_q} = SI_{MOE_j|TLM} * SI_{MOE_j, EDA_q} \quad (5.8)$$

Organizational errors are the consolidation of both TLM and MOE errors. As shown in Equation 5.8, the organizational error index is differentiated into two categories. First, the *top-level management index* ($SI_{MOEj|TLM}$) measures the level of top-level commitment to safety and resource allocation for safety measures. The TLM commitment to safety and resources has varying degrees of impact upon MOEs. In Equation 5.9, $SI_{MOEj|TLM}$ is the safety index of TLM's impact upon MOE_j Varying degrees of impact are measured by weighing the impact of five TLM factors:

Table 5.2: Documentation format of human errors and associated organizational errors for accident class n, consequence v_k, EDA_q, human factors, system factors, and environmental factors

Human Errors (HE_i)	know/ training/ exper (MOE_1)	maint-enance (MOE_2)	violation (MOE_3)	morale/ incentive (MOE_4)	job design (MOE_5)	regul/ policing (MOE_6)	operating policy (MOE_7)	comm/ info (MOE_8)	manning (MOE_9)	none (MOE_{10})
hum/syst interface (HE_1)	ξ_{11kq}	ξ_{12kq}	ξ_{13kq}	ξ_{14kq}	ξ_{15kq}	ξ_{16kq}	ξ_{17kq}	ξ_{18kq}	ξ_{19kq}	$\xi_{1,10kq}$
know/train/ exper (HE_2)	ξ_{21kq}	ξ_{22kq}	ξ_{23kq}	ξ_{24kq}	ξ_{25kq}	ξ_{26kq}	ξ_{27kq}	ξ_{28kq}	ξ_{29kq}	$\xi_{2,10kq}$
mntl/phys lapse (HE_3)	ξ_{31kq}	ξ_{32kq}	ξ_{33kq}	ξ_{34kq}	ξ_{35kq}	ξ_{36kq}	ξ_{37kq}	ξ_{38kq}	ξ_{39kq}	$\xi_{3,10kq}$
violations (HE_4)	ξ_{41kq}	ξ_{42kq}	ξ_{43kq}	ξ_{44kq}	ξ_{45kq}	ξ_{46kq}	ξ_{47kq}	ξ_{48kq}	ξ_{49kq}	$\xi_{4,10kq}$
job design (HE_5)	ξ_{51kq}	ξ_{52kq}	ξ_{53kq}	ξ_{54kq}	ξ_{55kq}	ξ_{56kq}	ξ_{57kq}	ξ_{58kq}	ξ_{59kq}	$\xi_{5,10kq}$
comm/inξo (HE_6)	ξ_{61kq}	ξ_{62kq}	ξ_{63kq}	ξ_{64kq}	ξ_{65kq}	ξ_{66kq}	ξ_{67kq}	ξ_{68kq}	ξ_{69kq}	$\xi_{6,10kq}$

where,

$$\xi_{ijkq} = \left\{ \xi_{HE_i, OE_j, EDA_q, HF, Syst, Env} \right\}_k$$

(1) *overall commitment to safety* (Q_1),
(2) *commitment to long term safety goals* (Q_2),
(3) *cognizance of problems* (Q_3),
(4) *competence to correct the problem* (Q_4), and
(5) *sufficient resources to correct problems* (Q_5)

such that,

$$
\begin{aligned}
SI_{MOE_1|TLM} &= \max\left\{\phi_{11}Q_1+\phi_{21}Q_2+\phi_{31}Q_3+\phi_{41}Q_4+\phi_{51}Q_5, \left(SI_{MOE_1|TLM}\right)_o\right\} \\
SI_{MOE_2|TLM} &= \max\left\{\phi_{12}Q_1+\phi_{22}Q_2+\phi_{32}Q_3+\phi_{42}Q_4+\phi_{52}Q_5, \left(SI_{MOE_2|TLM}\right)_o\right\} \\
&\vdots \\
SI_{MOE_j|TLM} &= \max\left\{\phi_{1j}Q_1+\phi_{2j}Q_2+\phi_{3j}Q_3+\phi_{4j}Q_4+\phi_{5j}Q_5, \left(SI_{MOE_j|TLM}\right)_o\right\} \\
&\vdots \\
SI_{MOE_9|TLM} &= \max\left\{\phi_{19}Q_1+\phi_{29}Q_2+\phi_{39}Q_3+\phi_{49}Q_4+\phi_{59}Q_5, \left(SI_{MOE_9|TLM}\right)_o\right\} \\
SI_{MOE_{10}|TLM} &= 1
\end{aligned}
\tag{5.9}
$$

where,

$$
Q_c = \begin{cases} 1 & \text{if "high" or "sufficient"} \\ -1 & \text{if "low" or "insufficient"} \end{cases}
$$

$$
\sum_a \phi_{aj} = 1 \qquad \forall j
$$

If the TLM factor is "high" or "sufficient", it adds to the safety index, however if "low" or "insufficient", it reduces that safety index. The weights can be thought of as the percent of impact upon MOEs by TLM factors. Since MOE_{10} represents no organizational errors, there is no impact of TLM on MOE_{10} thus the safety index is unchanged.

Second, the *middle-operator level management safety index* ($SI_{HE_i|MOE,EDA_q}$) is the sum of each organizational error's effect upon a particular human error "i" (HE_i). Each index associates the organizational error's effect upon human errors at the operator level. The minimum value of the impact of top-level management $\left(SI_{MOE_j|TLM}\right)_o$, is provided by the user and should be established such that $\left(SI_{MOE_j|TLM}\right)_o \geq 0$.

To determine the safety index for a particular HE as a result of the organizational errors (OEs), the safety index is determined by providing estimates of the relative effect of "good", "fair", or "poor" organizational error management. Figure 5.15 is a graphical display of how routine a safety index is obtained through a linearization technique and described in Equation 5.10.

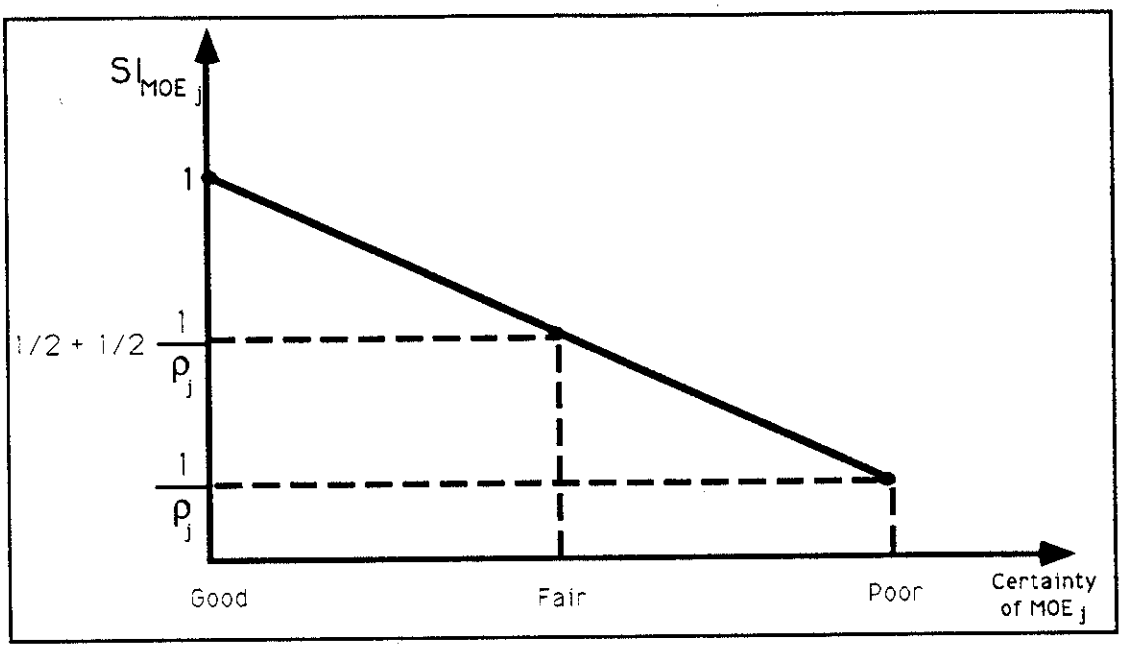


Figure 5.15 - Linearized measurement of middle-front line management index

$$SI_{MOE_j,EDA_q} = \begin{cases} 1 & \text{if "high"} \\ 1/2 + 1/2(1/\rho_j) & \text{if "moderate"} \\ 1/\rho_j & \text{if "low"} \end{cases} \qquad (5.10)$$

where ρ_j is the maximum degree by which MOEj is judged to be increased for EDA_q.

The human factor index described in Equation 5.5 is categorized into the product of a *stress index* ($SI_{Stress,EDAq}$) and a *routineness index* ($SI_{Routineness,EDAq}$) as shown in Equation 5.11. Stress and routineness are measured to assess the relative effect upon the safety of the system. The user judges the relative effect of "high" stress or routineness. Figure 5.16 is a graphical display of how the stress safety index is obtained through a linearization technique and shown in Equation 5.12. The index measuring routineness of the EDA_q is linearized and shown in Figure 5.17 and the formulation is described in Equation 5.13.

$$SI_{Hum\ factor,EDA_q} = SI_{Stress,EDA_q} * SI_{Routineness,EDA_q} \qquad (5.11)$$

$$SI_{Stress|EDA_q} = \begin{cases} 1 & \text{if "low"} \\ 1/2 + 1/2(1/\alpha) & \text{if "moderate"} \\ 1/\alpha & \text{if "high"} \end{cases} \quad (5.12)$$

where α is the maximum degree by which stress is judged to be increased for EDA_q.

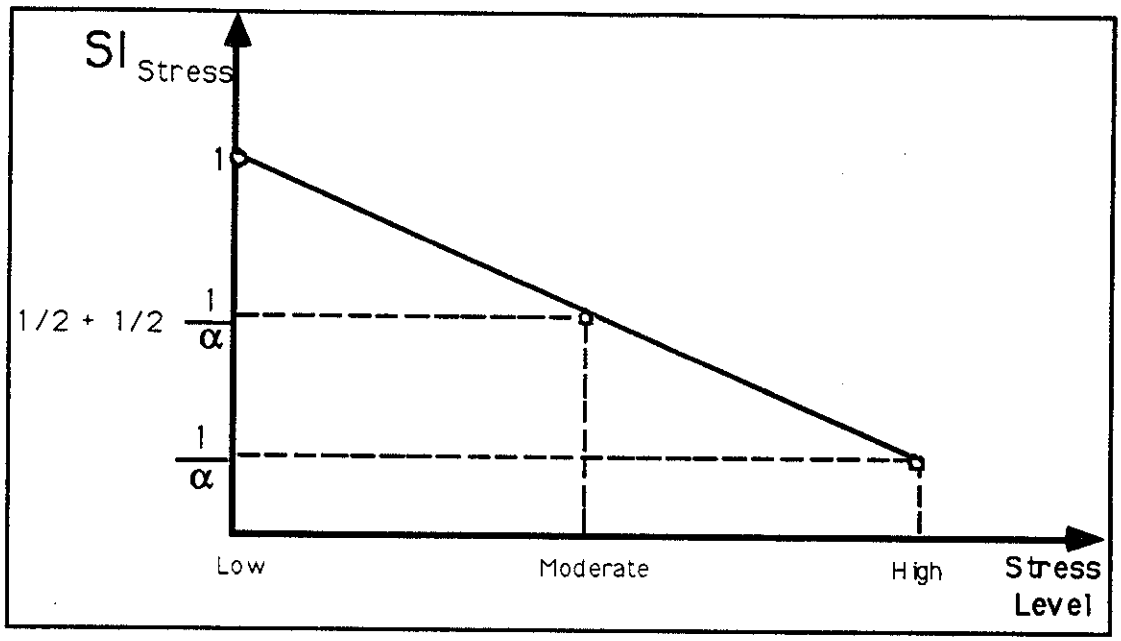


Figure 5.16 - Linearized measurement of stress

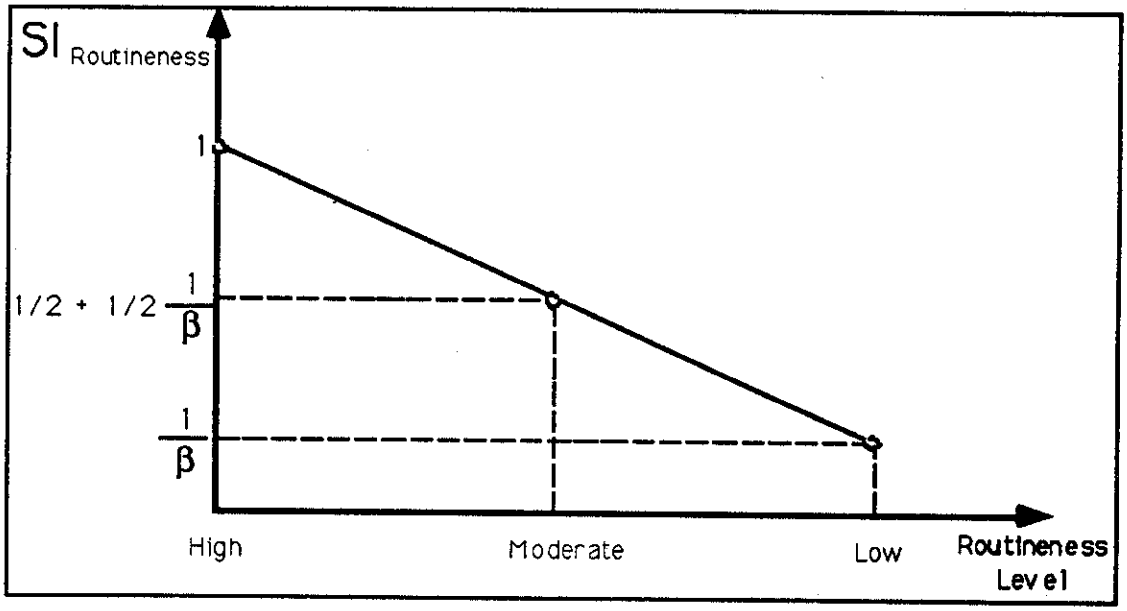


Figure 5.17 - Linearized index measurement of routineness

$$SI_{Routineness|EDA_q} = \begin{cases} 1 & \text{if "high"} \\ 1/2 + 1/2(1/\beta) & \text{if "moderate"} \\ 1/\beta & \text{if "low"} \end{cases} \quad (5.13)$$

where β is the maximum degree by which routineness is judged to be increased for EDA_q.

The *system safety index* ($SI_{System,EDAq}$) of Equation 5.5 measures the ability of the operator to properly acquire, assess, and act on information provided by the operating system. Similar to the quantitative calculation of stress and routineness, judgments are made as to the impact of system factors upon the overall safety index. The linearization is shown in Figure 5.18 and formalized in Equation 5.14.

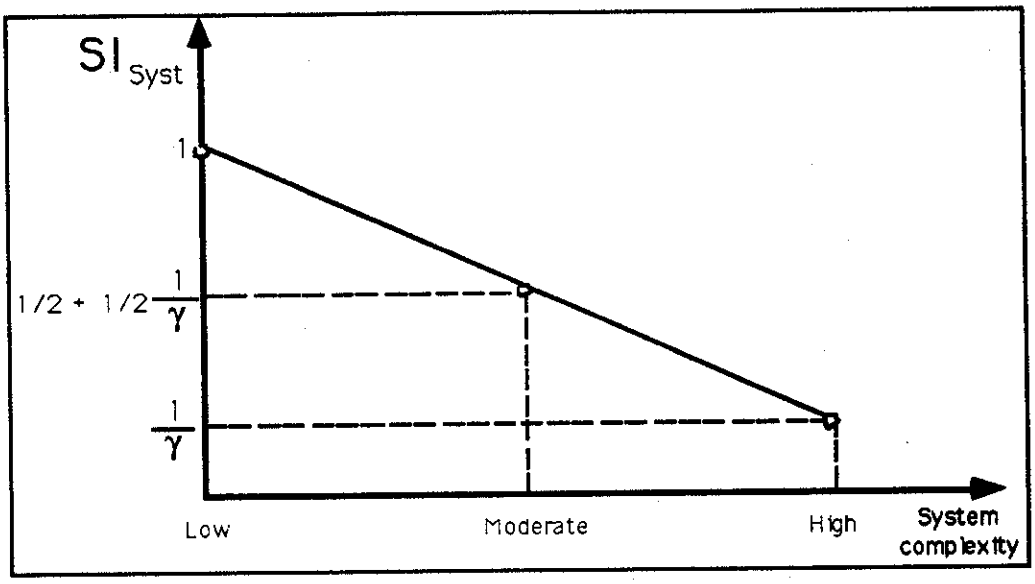


Figure 5.18 - Linearized measurement of system complexity

$$SI_{Syst|EDA_q} = \begin{cases} 1 & \text{if "low"} \\ 1/2 + 1/2(1/\gamma) & \text{if "moderate"} \\ 1/\gamma & \text{if "high"} \end{cases} \quad (5.14)$$

where γ is the maximum degree by which system complexity is judged to be increased for EDA_q.

The *environmental safety index* ($SI_{Environ,EDAq}$) in Equation 5.15 is the product of two indices: the *external operating condition impairment index* ($SI_{External,EDAq}$) and *internal operating condition impairment index* ($SI_{Internal,EDAq}$).

$$SI_{Environ,EDA_q} = SI_{External_u,EDA_q} * SI_{Internal_v,EDA_q} \quad (5.15)$$

The impacts of environmental factors in HESIM represent external and internal impairment contributors. Environmental factors impair the individual operator's ability to think and perform actions. Any combination of environmental factors may affect the abilities of the operator. However, any number of environmental factors may be the dominant contributors to errors. For example, fire and smoke may be impairing the abilities to evoke mitigation procedures. However, smoke may be the dominant environmental factor leading to errors by the operators due to the operators inability to breath correctly. It is at the discretion of the user to determine degree to which a single environmental factor, or any combination of factors, affects the environmental safety index. This may be performed by a linearization method similar to the safety indices developed for stress, routineness, and system complexity factors developed above. As shown in Figure 5.19, "high", "moderate", and "low" environmental impairment severity affect the accident contributors. Equation 5.16 is the linearization equation used to determine the environmental safety indices.

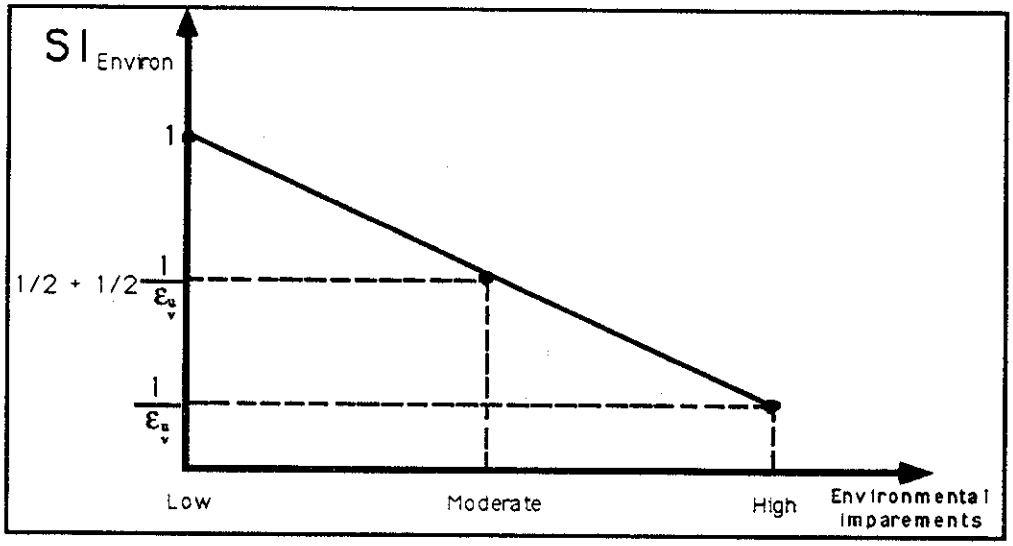


Figure 5.19 - Linearized measurement of environmental impairment factors

$$SI_{Environ\left\langle \frac{Ext_u}{Int_v} \right\rangle, EDA_q} = \begin{cases} 1 & \text{if "low"} \\ 1/2 + 1/2(1/\varepsilon_{u,v}) & \text{if "moderate"} \\ 1/\varepsilon_{u,v} & \text{if "high"} \end{cases} \qquad (5.16)$$

where ε is the maximum degree by which external environmental factor u (ε_u) or internal environmental factor v (ε_v) is decreased for EDA_q.

5.7 FUTURE DATA ANALYSIS: THE HOEDQS

The development of the HESIM algorithm as a means for quantifying the impacts of human errors as a result of an error solicitor (event, decision, or action) in the previous chapter. As observed in Figure 5.13, human error solicitors are either heightened or re-

duced by organizational-regulatory errors. The HOE database development framework is used to associate the front-line operator errors (human errors) and middle-front-line management (organizational-regulatory errors) under the operating conditions described in the prior section (human factors, system complexity, and environmental contributors).

The database system, the *Human and Organizational Error Data and Quantification System* (HOEDQS) serves two purposes. First, it provides a basis from which to obtain quantitative measurements for the HESIM described in the previous section. The HOEDQS allows the user to incorporate the data being collected-updated the expert judgment in generating quantitative measurements for organizational, human factors, system, and environmental contributors. Second, the database system provides the user friendly environment from which to generate probabilistic measures of human and organizational errors to marine casualties and near misses. As discussed in Chapter 2, the lack of accurate data for marine casualties and near misses has made it difficult to generate reliable probabilistic risk analysis models. The HOEDQS provides the framework from which to collect casualty and near miss data.

As data becomes available, less reliance on expert opinion and judgment is required for the quantitative development and a greater reliance upon the data will lead to better quantitative measurements. This will also lead to a reduction of the need to rely upon the HESIM to generate quantitative data. The remainder of this chapter is dedicated to an explanation of the HOEDQS data collection procedure and the quantitative measurement. A user guide explanation of how to operate the HOEDQS program is provided in Appendix 3.

5.7.1 The Data Collection Procedure

The following is a procedure by which to collect and document HOEs for marine casualties and near misses.

(1) *Identify the class of accidents for which the casualty data is to be collected* (e.g. collisions, groundings, offshore production fires or explosions, crane accidents, etc.). Separate database are collected for each accident class of interest.

(2) *Identify casualties by the degree and type of consequences.* This may be established by first identifying what are considered "small", "moderate", "large" and catastrophic consequence levels and categorize consequences on this basis. The consequence levels are identified at the user's discretion. In addition, the user identifies the intervals of consequences for which data is compiled. For example, a separate database can be compiled of HOE contributors to tanker load or discharge spills that are: (1) less than 10 barrels, (2) between 10 and 100 barrels, or (3) greater than 100 barrels. By categorizing casualties by consequence level, it may allow the users to identify particular trends that may differentiate between low and catastrophic consequence casualties.

(3) *Establishing the stage of occurrence of contributing factors to the accident or near miss sequence.* The casualty stages: underlying or contributing, direct, and compounding were discussed in Chapter 4. It is the responsibility of the user to define underlying direct, and compounding stages to assure error data is categorized into the appropriate casualty stage (see case study examples in Chapter 7).

The HOEDQS provides a format for the user to first identify a *primary* EDA at each accident stage. In addition, the user has the option of including *associated* accident events, decisions, and actions. Associated EDAs are relevant

to the primary EDA. For example, a primary underlying EDA for a tanker grounding would be the vessel deviating from a traffic separation scheme (TSS). Associated underlying EDAs could be insufficient monitoring (act of omission) and an improper radar signal (see tanker collision-grounding model in Chapter 7).

(4) *Determine contributing human factor, system and task complexity factors related to the event, decision, or action being performed.* For each EDA there could be related human factors, task, or system complexities that contribute to the casualty. In the HOEDQS, the user has the option of including human factor, task, and system complexity in the database. For example, the vessel deviating a TSS in Alaska's Prince William Sound at night in the winter could be considered either "moderate" or "high" task complexity while performing the EDA during daylight in the summer may be considered as "low" task complexity. In addition, deviating the TSS may be a routine operation, but environmental factors such as ice in the TSS or the time of day in which the operation is performed, may lead to a higher level of stress for the operators.

(5) *Establish the environmental impairment contributor associated with the event, decision, or action that may have induced human and organizational errors.* Each external and internal environmental impairment contributor presented in Table 3.1 is included in the HOEDQS program allowing the user the ability to input that factor as an error contributor.

(6) *Identify the contributing top-level management factors for the event, decision, or action performed that may have had a direct impact upon human and or mid-level/ront line management errors.* The HOEDQS user has the option of inputting their assessment of the impact of TLM factors on the accident scenario described previously in this chapter. Top-level management factors measured are overall commitment to safety, commitment to long term safety goals, cognizance of operational problems, competence to address the problems, and sufficient resources assigned to safety issues to correct problems.

(7) *Identify the contributing human and organizational errors at each stage of the accident sequence and relative certainty of joint human error and mid-level - front line management error occurrences.* The joint occurrences are defined as the influence between a front-line operator error (HE_i) and an organizational error (OE_j) for the EDA under the task, system, human factor, and environmental conditions. As a result of the complexity of any accident or near miss event, the HOEDQS allows the user a level of flexibility in associating the joint occurrences of human and organizational errors. The user is allowed to input whether they believe there is a "high", "moderate", or "low" certainty of joint occurrence of a particular HE and OE. When inputting accident data the following guidelines for determining error certainty levels are as follows.

   (i) *High certainty of joint occurrence*: The accident-near miss investigator has direct proof or evidence of the incidence of a particular HE occurring at the front line level as a result of a particular MOE.

   (ii) *Moderate certainty of joint occurrence*: The accident-near miss investigator has reasonable proof (direct or indirect) of the incidence of a particular HE occurring at the front line level as a result of a particular MOE.

(iii) *Low certainty of joint occurrence*: The accident-near miss investigator has indirect proof or limited reason to suspect an occurrence of a particular HE at the front line level as a result of a particular MOE.

5.7.2 Human Error Probabilities Under Varying Operating Conditions

Once a sufficient quantity of data has been collected, measurements can be made to determine "weighted" probabilities of front line human errors as a result of varying operating conditions (organizational errors, system and task complexity, human factors, and environmental operating conditions). The "weighted" probability, shown in Equation 5.17, is determined using the same method as that for producing Equation 5.6, by averaging across the weighted frequencies of joint occurrences between MOEs and HE's under all external operating conditions, human factors, and system complexity.

$$\tilde{P}_k[HE_i, OE_j, HF, Syst, Env_{n1}, \ldots, Env_{np}, EDA_q] = \left\{ f_{HE_i, OE_j, EDA_q, HF, Syst, Env} \right\}_k$$

$$= \frac{1}{m} \sum_m \left\{ \xi_{HE_i, OE_j, EDA_q, HF, Syst, Env} \right\}_{km} \tag{5.17}$$

Using Baye's Rule in Equation 5.18 one can solve for the probability of human error given organizational errors, system and task complexity, human factors, and environmental operating conditions (Equation 5.18a). The conditional "weighted" probability of human error shown on the left hand side (LHS) of Equation 5.18a is used for the quantification measurements described above.

$$\tilde{P}_k[HE_i, OE_j, HF, Syst, Env_{n1}, \ldots, Env_{np}, EDA_q] =$$

$$\tilde{P}_k[HE_i | OE_j, HF, Syst, Env_{n1}, \ldots, Env_{np}, EDA_q] \tag{5.18}$$

$$* \tilde{P}_k[OE_j, HF, Syst, Env_{n1}, \ldots, Env_{np}, EDA_q]$$

or,

$$\tilde{P}_k[HE_i | OE_j, HF, Syst, Env_{n1}, \ldots, Env_{np}, EDA_q] =$$

$$\frac{\tilde{P}_k[HE_i, OE_j, HF, Syst, Env_{n1}, \ldots, Env_{np}, EDA_q]}{\tilde{P}_k[OE_j, HF, Syst, Env_{n1}, \ldots, Env_{np}, EDA_q]} \tag{5.18a}$$

5.8 RISK INDEX COMPARISON TO CASE HISTORY EXAMPLES

The final step in the model development procedure is to relate the safety index evaluation to the overall reliability of the operating system. Figure 5.20 provides an overview of the HOE evaluation procedure. Step 1 entails the system analysis procedure, as described in Chapter 4, used to draw out the particular human, organizational, system, procedures, and environmental contributors to an accident scenario. The modeling procedure described

was to use influence diagrams to develop an accident template that retains the primary causative mechanisms to an accident scenario yet does not entail many of the unique characteristics of the casualty being modeled.

For Step 2, as proposed in this chapter, the HESIM was proposed as a quantitative measuring procedure that incorporates both available accident data and heuristic judgments. As data becomes more available, there is a reduction of reliance upon judgments and experiences and a greater reliance is placed upon objective data to generate human error related probabilities (e.g. HOEDQS).

Step 3 entails using the safety index evaluations for both calibrating and confirming the HESIM procedure. Historical failure rates for catastrophic events are used for confirmation of the modeling procedure and the HESIM is used to ensure that the quantitative modeling procedure is consistent with case study analyses. Once the safety (or risk) indices are evaluated for the HOEs using the HESIM, they are input into the influence diagram template model. An overall safety index is calculated for the target failure event being modeled (e.g. grounding or collision for a tanker, loss of fuel containment on production platform) such that:

$$P_f = \text{Probability of "Activity" results in undesirable outcome}$$

As shown in Figure 5.21, the safety index is then compared to the probability of failure for that particular accident event. This procedure is then repeated for a sufficient number of cases to determine a general range for the functional relationship between the safety indices and the failure event probabilities (Figure 5.22).

As shown in Figure 5.22, a risk meter can be developed that compares the safety index and the reliability of the operational system. The risk of failure can be categorized into "low", "moderate", and "high" intervals. The threshold values between high, moderate, and low (or unacceptable, marginal, and acceptable) risks are dependent upon the failure event, the consequences of that failure, and society's willingness to accept the risk. For example, a high level of risk for a tanker grounding in Prince William Sound, an environmentally sensitive area, may not be as high as a spill in the Gulf of Mexico off of Louisiana. A further discussion of criteria to consider for risk is included in Chapter 6.

Comparison between the safety index-reliability curves and probability-consequence curves for undesirable outcomes is performed to determine the relative risk to the undesirable outcome being modeled. This is expressed diagramatically in Figure 5.23 where the risk index-reliability curve is compared with the reliability-consequence curve. Further discussion of the reliability consequence curves and risk acceptability are discussed in Chapter 6.

Further evaluation of the models are performed to assess management alternatives to prevent and mitigate the impacts of HOE related factors. This is performed to determine if the impact upon the system will increase the reliability of the system such that the risk becomes acceptable. This can be expressed diagramatically in Figure 5.23 where the risk index-probability curve is compared with the probability of failure acceptability curve.

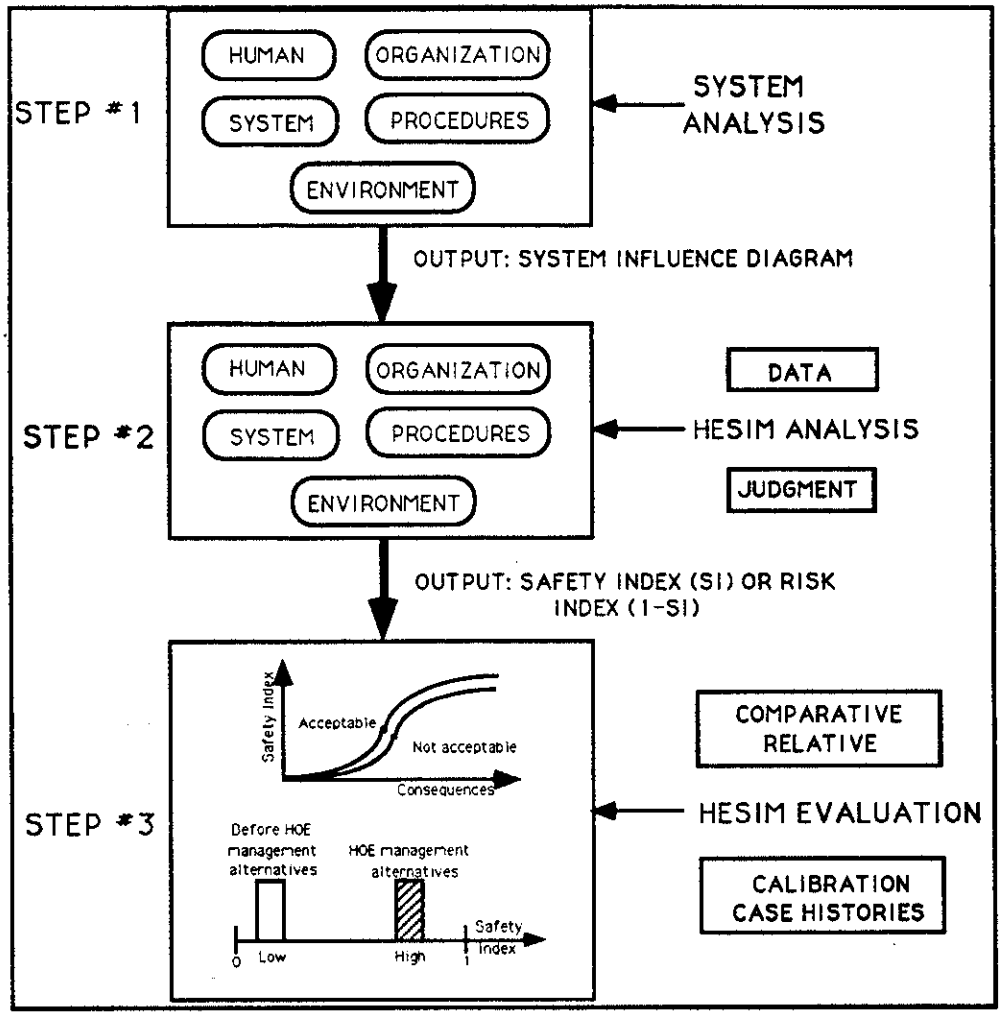


Figure 5.20 - HOE analysis procedure

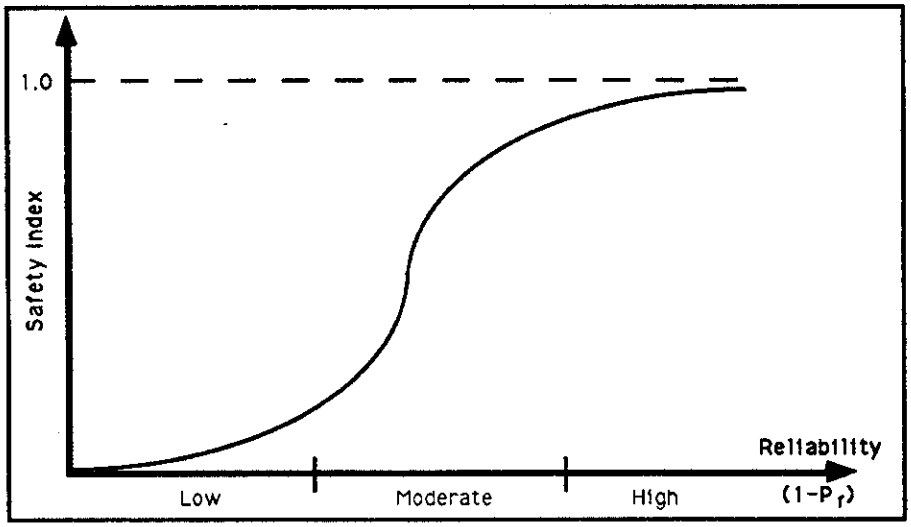


Figure 5.21 - Probability-risk index relation curve

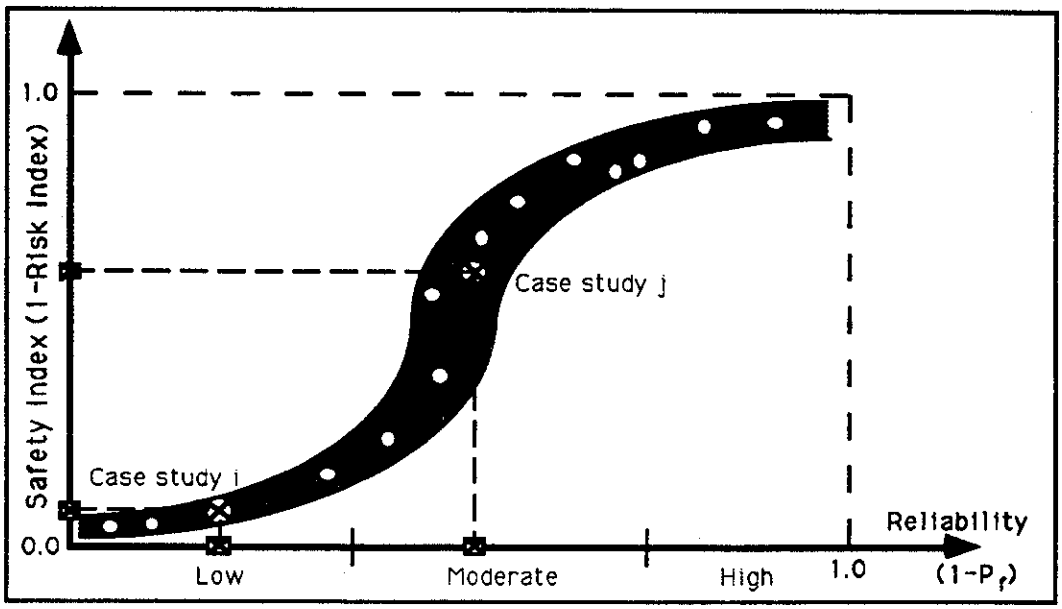


Figure 5.22 - Safety index-reliability curves

There is a six step approach to confirmation of the modeling procedure and the HESIM to both assess the risk of a particular undesirable target event and generate the safety-reliability curves shown in Figure 5.23. The approach is as follows:

(1) Determine the threshold probabilities between acceptable, marginal, and unacceptable risks for the operation being modeled. These can be done through judgments, historical data comparison, financial settlements for prior casualties, etc. (see Chapter 6).

(2) Determine the probability of the target event being modeled through judgment or historical data. For example, prior to the grounding of *Exxon Valdez*, a spill of the magnitude observed for that casualty was considered a 1 in 241 year event [Davidson, 1990].

(3) Using the post-mortem study data, calculate the human error safety indices (risk indices) under the specific operating conditions using HESIM. Input the human error indices into the influence diagram template model representing the particular characteristics of the scenario being modeled.

(4) Calculate the risk index for the undesirable target event by reducing the influence diagram template model. Reducing influence diagrams is further described in Appendix 3 and the *InDia*™ user guide [Decision Focus Incorporated, 1991].

(5) Compare the results of the risk index with the target event probability. If the risk index and probability of the target event are consistent with case study implications, continue.

(6) If the safety index and probability of failure are inconsistent, calibrate the HESIM to attain consistency of results. This can be conducted by reexamining the impact of error contributors or further detailing the model.

(7) Repeat Steps 1-6 for other case histories to attain reliable results.

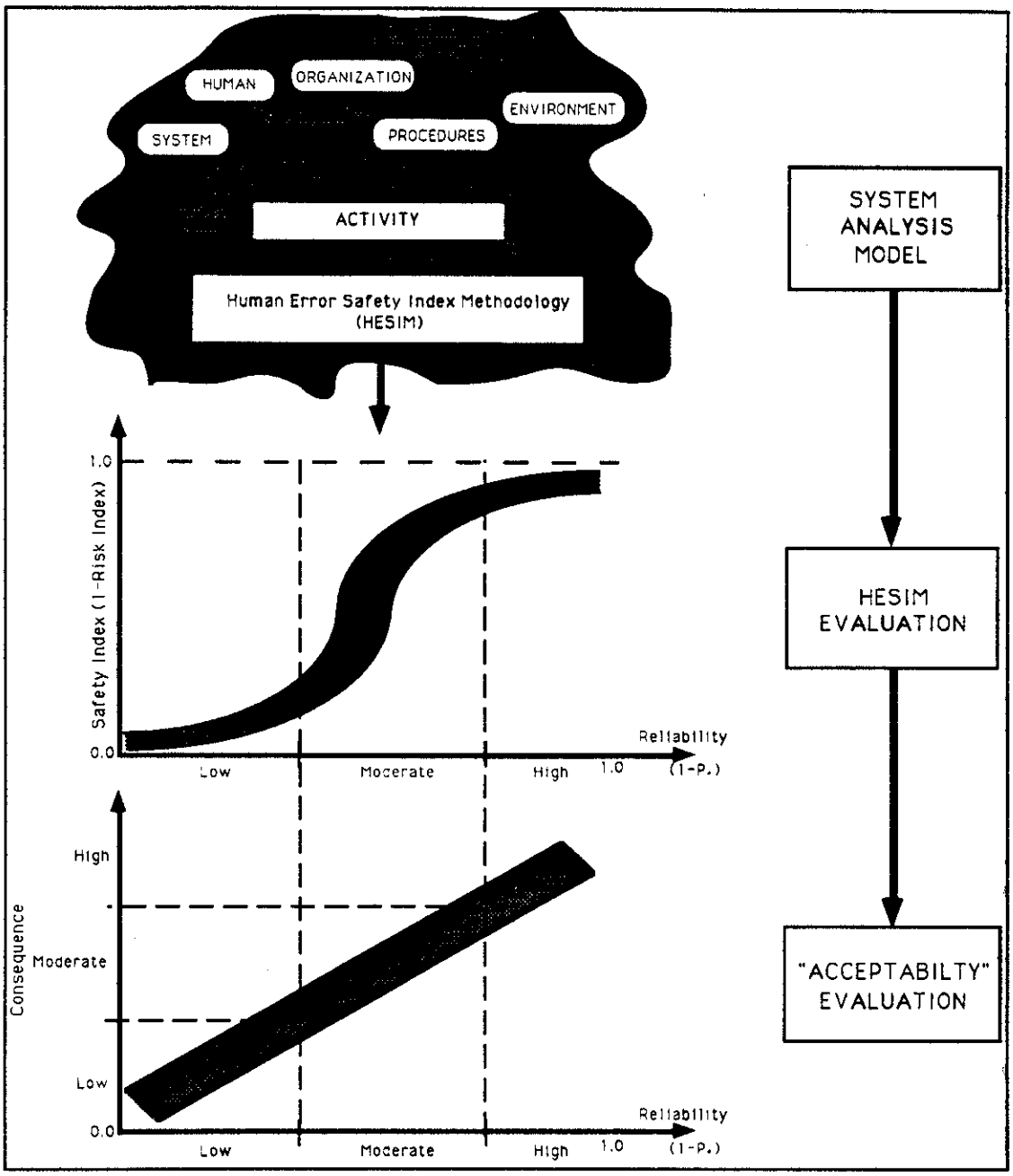


Figure 5.23- Safety index-probability-consequence curve comparisons for acceptable risk determination

Case study based confirmation of the HESIM procedure is provided in Chapter 5.

5.9 SUMMARY

As a result of the limited data available documenting the impacts of human errors on marine related casualties, it is important to develop a quantitative estimating procedures. Three procedures were described that incorporate varying degrees of HOE related information of the operating system. Probability encoding was described and the associated biases involved in that modeling procedure. The *Human Error Safety Index Method*

(HESIM), was introduced as a methodology for measuring the impact on human and organizational errors as a result of accident solicitors (events, decisions, or actions).

The database system, the *Human and Organizational Error Data and Quantification System* (HOEDQS) serves two purposes. First, it provides a basis from which to obtain quantitative measurements for the HESIM described in the previous section. The HOEDQS allows the user to incorporate the data being collected-updated. Second, the database system provides a user friendly environment from which to generate probabilistic measures of HOEs to marine casualties and near misses.

Once quantitative measurements of human errors are made using the HESIM procedure, the error indices are then input into the template diagram and the template is then reduced to determine the safety index for the events of interest. These indices are then compared on a linear scale to the failure probabilities so calibration between safety indices and probabilities of failures can be performed.

As data becomes available, lesser reliance on expert opinion and judgment is required for the quantitative development and greater reliance upon the data will lead to better quantitative measurements. This will also lead to a reduction of the need to rely upon the HESIM to generate quantitative data.

The strength of the data quantification system is that it is self correcting and has the capabilities of being updated and refined. The HESIM is used to assist in determining the impacts of organizational, system and task complexities, stress, routineness, and environmental conditions upon human errors and their effects upon increasing the operational risk. Error frequencies are updated using the HESIM and HOEDQS and are then used to update the failure event index. The failure event risk index is then matched against the failure probabilities for that event. A functional relation between the risk index and probability of the accident event is then determined. This allows for forecasting of the risk of failure events for future operations under various human operator conditions to determine if these operational conditions lead to an acceptable level of risk.

(3) *Continuous collection and assessment of human error data to monitor impacts of error management systems.* Direct data analysis is the most effective method of determining HOE management programs. The HOEDQS, an HOE data collection procedure is described in Chapter 5. As the data is collected and updated, the effects of management alternatives are measured with a greater level of accuracy.

In Chapter 5 the HOEDQS human error database system that allows users to document the effects of particular types of human errors in accident scenarios was introduced. As described in Chapter 3, safety management systems are in a constant state of change in unison with changes in the organization. It should be realized that an organization's resistance to safety problems is also in a constant state of change. The HOEDQS is a tool that can assist users in monitoring both trends in casualties near misses and in assessing the impact of HOE management alternatives once implemented.

6.2.2 Operational Change and Error Tolerant Systems

Heuristic judgment in determining direct and indirect effects of HOE management alternatives effect the structure of the model through the addition of *error inhibitors*. Error inhibitors are defined as changes in management, operations, or procedure that can influence the incidence of human and organizational errors. As shown in Figure 6.1, the error inhibitor may be either explicitly accounted for within the influence diagram by defining a node and directly accounting for the effects on other nodes (solid arrows). Or, error inhibitors may be implicitly accounted for by not directly defining a node, but through modifications in the quantitative distributions of explicitly accounted for factors (dotted arrows) (see examples in Chapter 7 for both explicit and implicit models). As observed, error inhibitors can affect human errors factors but also other EDAs within the model.

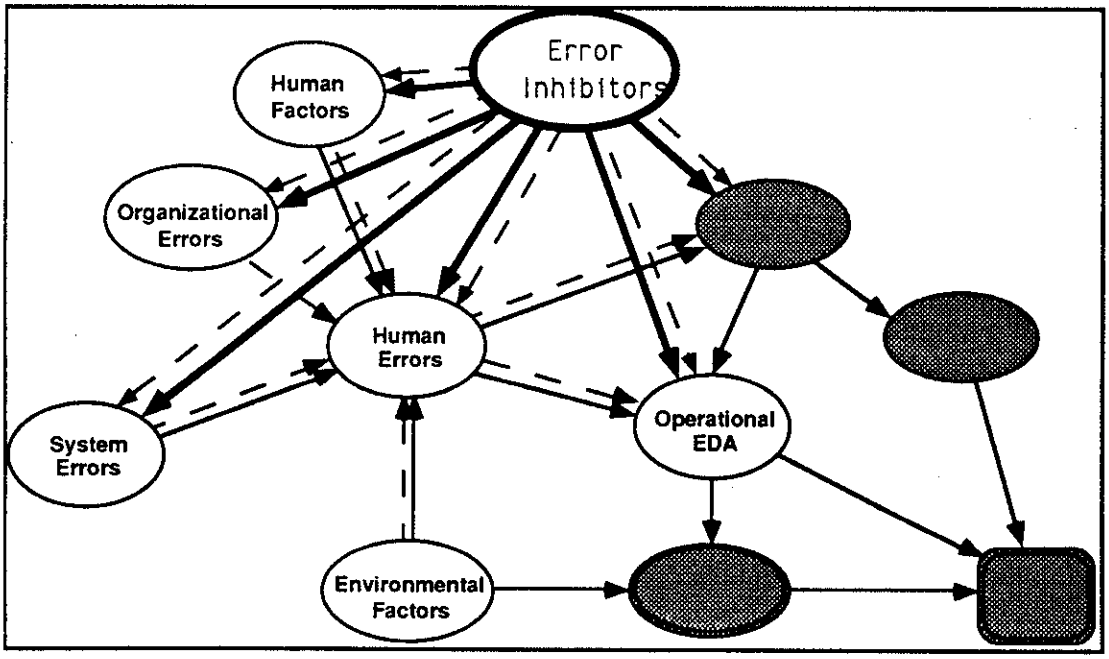


Figure 6.1 - Effects of error inhibitors upon influence diagram models

As an illustration, Figure 7.6 is an influence diagram model for tanker grounding or collision that has been modified to incorporate the impact of tug escorts. The tug escort influences both the structure of the model and the error frequencies. For example, the tug influences the frequencies of groundings by providing assistance should the vessel become incapacitated. In addition, the tug support can influence tanker crew errors by having additional personnel monitoring the vessel's path.

The next step is to determine the effects of the operational error inhibitors by using the probability encoding and the HESIM techniques described in Chapter 5. If error tolerant systems have been implemented in similar industries, comparative analysis with these industries can assist decision makers in assessing the effects of various management alternatives.

6.3 HOE MANAGEMENT DECISIONS - EVALUATING THE RISK

6.3.1 What is Safe Enough?

Though short term financial and operational cost effective HOE management alternatives should be considered, there are additional factors that have a long range impact on the costs of operating. These long term affects can have substantial long term effects upon operations and should be addressed in the decision process.

(1) *Changing attitudes towards risk.* The uncertain nature of changes in attitude towards risk can have a major impact upon operational policy. A single catastrophic accident can have long range effects upon regulatory policies and public perception of risks.

(2) *Regulatory climate.* As a result of risks (real and perceived), better technologies, and high profile casualties, regulatory agencies are continually updating regulation to be consistent with the means by which to reduce casualties. It is imperative for decision makers to keep pace with trends to allow for them to have a greater say in how new regulations are implemented and allow for easier transitions to comply.

(3) *Risk and perceived risk.* As the public becomes more familiar with various marine operations as a result of catastrophic accidents and perceived risks of catastrophic accidents, there are growing pressures to police and regulate those operations. For example, the *Three Mile Island* nuclear disaster led to more stringent nuclear facility regulation and led many communities to demand that no nuclear facilities be constructed in or around their communities. Though few nuclear disasters have occurred, there is a "no accident" policy for nuclear facilities given the catastrophic nature of accidents. Many people demanded sweeping changes of tanker operations after the grounding of *Exxon Valdez*. The passage of *OPA 90* and other local legislation has led many operators to drastically change operational procedures to accommodate those changes (see Chapter 7).

(4) *Costs of catastrophic accidents.* Many decision makers do not wish (consciously or sub-consciously) to believe that a worst possible case casualty could happen to them. Quantitative risk analysis has a history of accounting for are performed that can show particular catastrophic scenarios as "extremely improbable" [Paté-Cornell, 1992].

6.3.2 Quantifying Risk

There are a number of sources that look into risks evaluation from quantitative analyses. The general quantitative measure of risk can be described as the product of the probability of a degree of failure and the consequences of that degree of failure. Both historical utility based approaches and the standard of practice measuring techniques have been proposed and discussed for marine systems [Bea, 1989, 1990; Flint and Baker; 1976; Gale, 1993; Moan, 1983; Paté-Cornell and Bea, 1989; Stahl, 1986, Siktec, 1986]. Two general approaches to defining acceptable levels of risk as defined by Bea (1990) are *experience evaluations* and *utility evaluations*. It has been shown that each approach will provide similar results that allow decision makers to make consistent decisions (Bea, 1990).

6.3.2.1 Experience evaluations

At the initiation of any new activity, one generally associates a higher level of risks since the activity, technology, and operations are new and untested. As people (directly and indirectly involved with the activity) become more aware, involved, and experienced with the activity, there will be a reduction in the tolerance level of acceptance for risks in that technology (Figure 6.2). As shown in Figure 6.3, the reliability of major drilling and production platforms has increased considerably through time with new technologies and experiences. Higher levels of risk were acceptable for U.K continental shelf activities from the 1960's through the early 1980's [Carson, 1982]. However, such accidents as the *Exxon Valdez* and *Piper Alpha* disasters have changed the public's perception of acceptable risks.

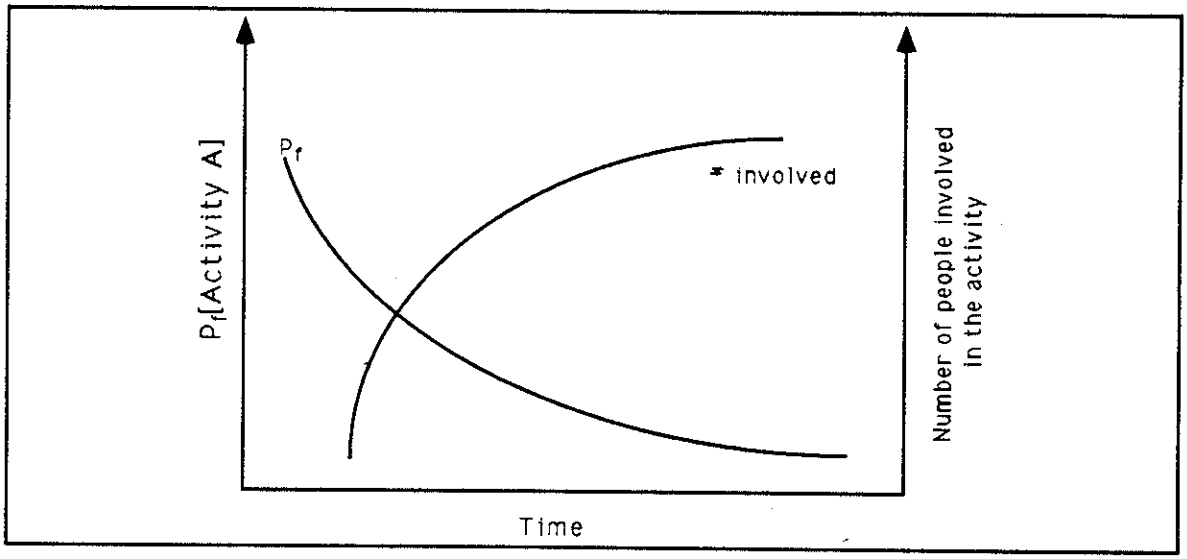


Figure 6.2 - Probability of failure and number of members versus time for an activity

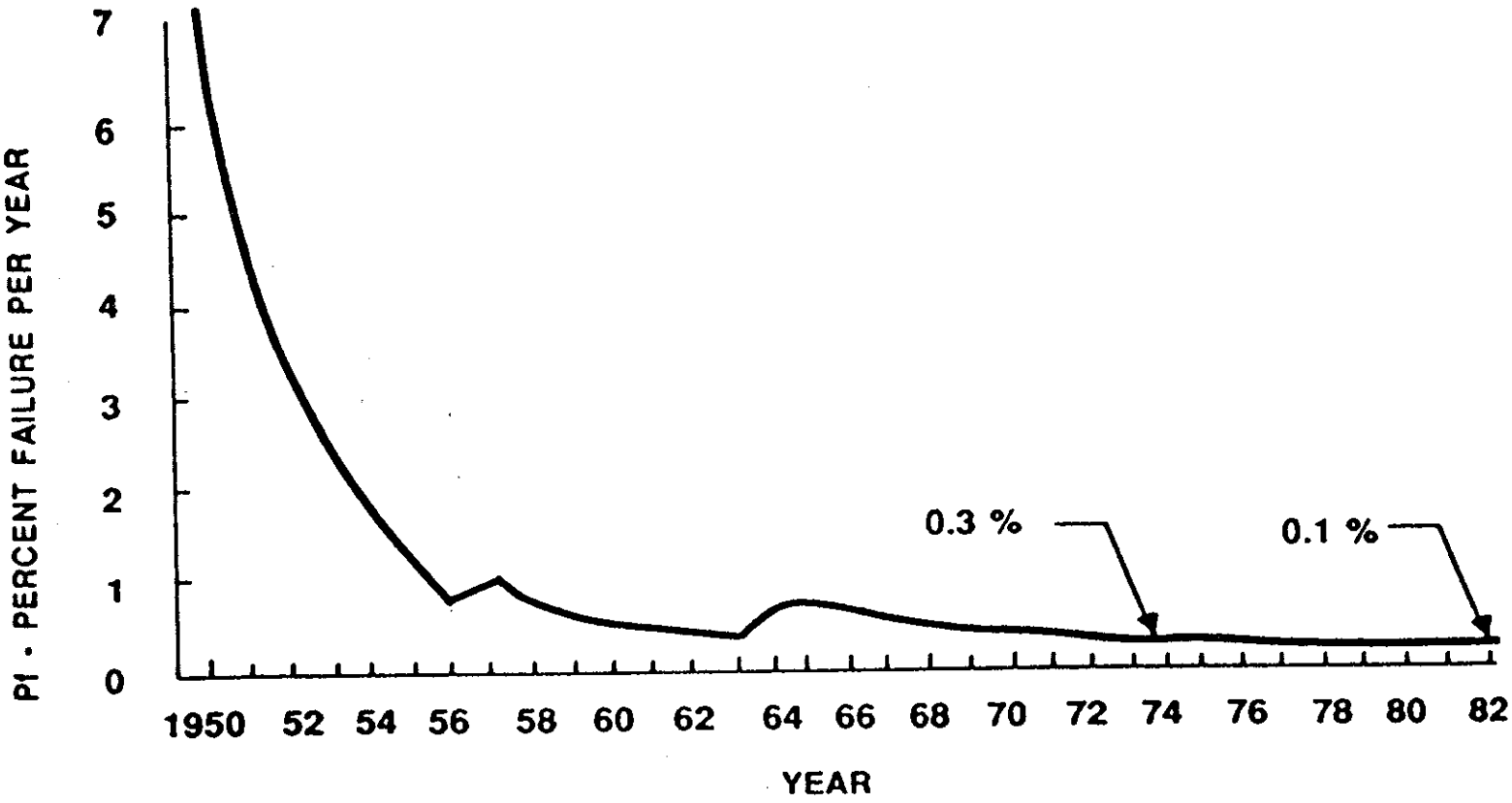


Figure 6.3 - Reliability of major drilling and production platforms in the Gulf of Mexico subjected to hurricanes during the period 1950-1981

Figure 6.4 is a descriptive diagram that shows the consequences of failure versus the probability of that failure. For low consequence failures, we are more likely to accept higher frequencies of failure. However for high consequence failures, we wish to see a substantially smaller frequency of failure. This is the case for "acceptable risk" and "marginally acceptable risk" curves. The positioning of these curves are established by the industry, society, and individuals who make trade-offs between consequences and risks [Bea, 1990; Whitman, 1984]. The lines in Figure 6.4 are based on annual costs, insurance and legal payments.

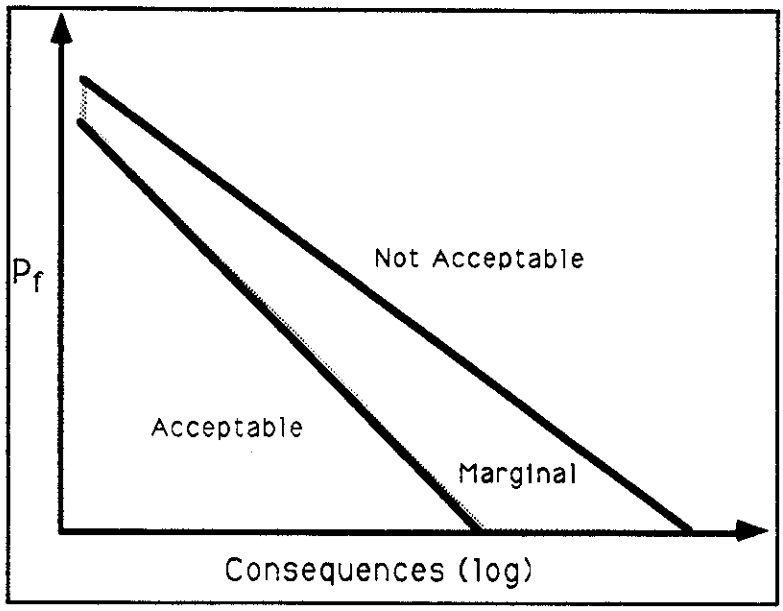


Figure 6.4 - Consequence vs. probability of failure acceptability regions [Bea, 1990]

For example, USCG statistics have determined that the ratio of oil spilled per gallon transported for tankers was 3.32×10^{-5} and for barges it was 1.73×10^{-5} between 1974 and 1978 [National Research Council, 1981, 1991]. In the 1980's, the annual average loss for tankers and barges combined was 1.5×10^{-5}. The average rate loss had decreased from the 1970's to 1980's however, society's willingness to accept the risk has dropped, particularly in wake of such catastrophic disasters as *Exxon Valdez*. In comparison to other industries, the ratio of oil transported and spilled for the oil pipeline industry is 1.5×10^{-5}, the probability of landings being aborted is less than 1×10^{-7} [National Research Council, 1991].

6.3.2.2 Utility evaluations: Cost-benefit analysis

The most common utility evaluation is cost-benefit analysis. The costs and benefits may be evaluated in terms of economical, fatal accident or injury rates, loss of hydrocarbons, probabilities of catastrophic failure events or any other means identified by the user as a measure of gain or loss.

In cost-benefit analysis, alternatives are evaluated by determining the net reduction in costs to the system. The impact of alternative set j (A_j) can be described by Equation 6.1. Alternative set j may be one or more management alternatives implemented to reduce the

impact of HOE. The alternatives are the net benefit of implementing A_j. which is the difference between implementing no alternatives and the cost of implementing A_j.

$$NB_{Aj} = C_o - B_{Aj} \tag{6.1}$$

where,

A_j = Set of HOE management alternatives j

$B_{Aj} = C_{Aj} - \sum_{i=1}^{n} C_{Aji}$

= Cost of implementing A_j for each management alternative i which is part of alternative set j.

C_o = Cost of particular accident classes when implementing no alternatives j.

C_{Aj} = Cost of particular accident class when implementing alternatives j.

B_{Aj} = Benefit of implementing A_j

NB_{Aj} = Total net benefit of A_j

As a measure of the net benefits, the expected costs and benefits can be used as shown in Equation 6.2. The standard deviation of net benefits should also be measured as a determinant to the variability in costs, benefits, and net benefits to the decision makers. Equation 6.3 provides the standard deviation of net benefits assuming independent, normally distributed variables of implementing no alternatives (C_o) and benefits of management alternatives (B_{Aj}). The accident costs are dependent upon such factors as casualty severity, sensitivity of the environment to accidents, casualty location, legal costs, social costs, costs to business, etc. Similarly, benefits also vary dependent upon the differences in costs of implementing those HOE management alternatives. These changes can affect production, manpower, demand high levels of expertise, and other important resources.

$$\overline{NB}_A = \overline{C}_o - \overline{B}_A \tag{6.2}$$

$$\sigma_{NB_A} = \sqrt{\sigma^2_{C_o} + \sigma^2_{B_A}} \tag{6.3}$$

As shown in Figure 6.5 to reduce the probability of failure, the initial cost are greater to develop a system to obtain a higher degree of safety. On the other hand, if little initial costs are applied to the system, the probability of failure will be greater. Future costs are lower for low probability events since the expected costs of failure are likely to be observed. Higher future costs of failure are observed if failures are observed as a result of a need to correct the problems. Since there is a degree of uncertainty as a result of cost uncertainties as a result of variability in costs of design, construction, installation, and operations, a range of values are represented for both initial and future cost functions.

The total expected cost of failure to the system is what is of interest. As expressed in Equation 6.4, the expected cost of failure event k is the product of the probability and the consequence of event k. The total expected cost is expressed in Equation 6.5 as the sum of expected initial costs and expected future costs.

$$E[C_k] = P_k * C_k \tag{6.4}$$

$$E[C_{total}] = E[C_{initial}] + E[C_{future}] \tag{6.5}$$

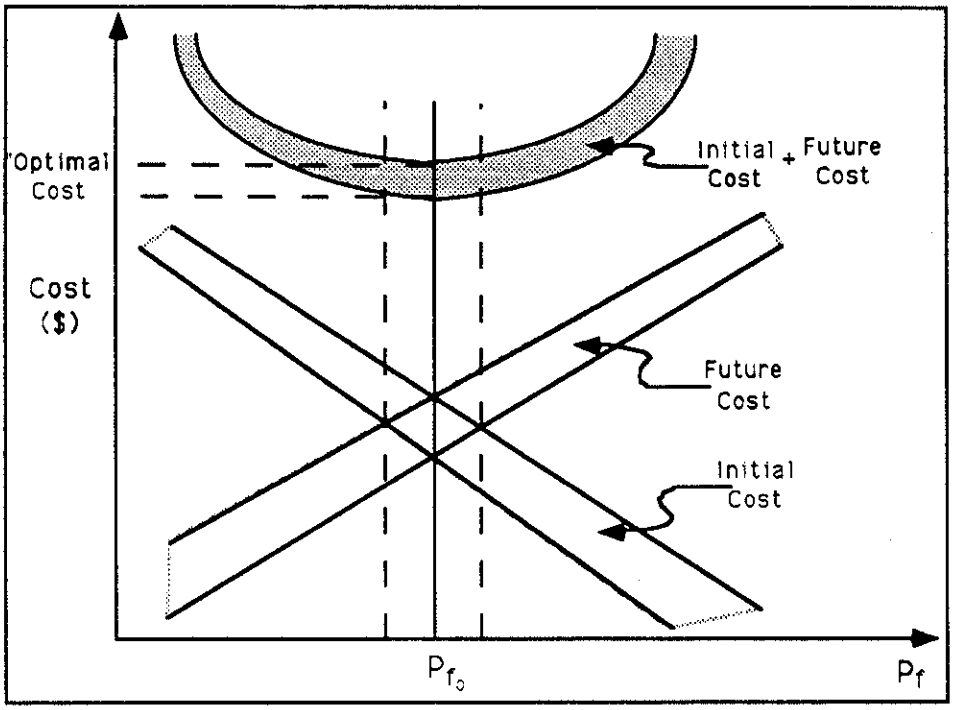


Figure 6.5 - Probability of failure versus cost optimum [Bea, 1990]

Expected future costs can be discounted to present value by multiplying the expected cost by a present value function as shown in Equation 6.6. The present value function (PVF) is a function the discount rate i, the useful lifetime of the marine structure or operation. As observed in Equation 6.7, any future costs can now be expressed in a present value costs.

$$PVF = \frac{1-(1-i)^{-L}}{i} \tag{6.6}$$

$$E[C_{future_k}] = P_{future_k} * C_{future_k} * PVF_k \tag{6.7}$$

Bea (1990) expresses the cost associated with marine system development as being related linearly to the logarithm of the probability of serviceability loss as shown in Equation 6.8. The initial cost is a function of the product of the probability failure (P_f) and the slope of the cost curve (C). By substituting in Equation 6.7 and Equation 6.8 into Equation 6.5 and taking the differential with respect to the probability of failure, one is

able to obtain the optimal (acceptable) probability of failure (P_{fa}) and the associated cost as shown in Figure 6.5. This can be expressed by Equation 6.9.[1]

$$C_{initial} = C_o + C * \log_{10}(P_{failure}) \tag{6.8}$$

$$P_f = \frac{0.435}{PVF * CR} \tag{6.9}$$

Given that the "marginal" probability of failure is twice the acceptable marginal of failure ($P_{fm} = 2P_{fa}$), the results can be portrayed in Figure 6.6.

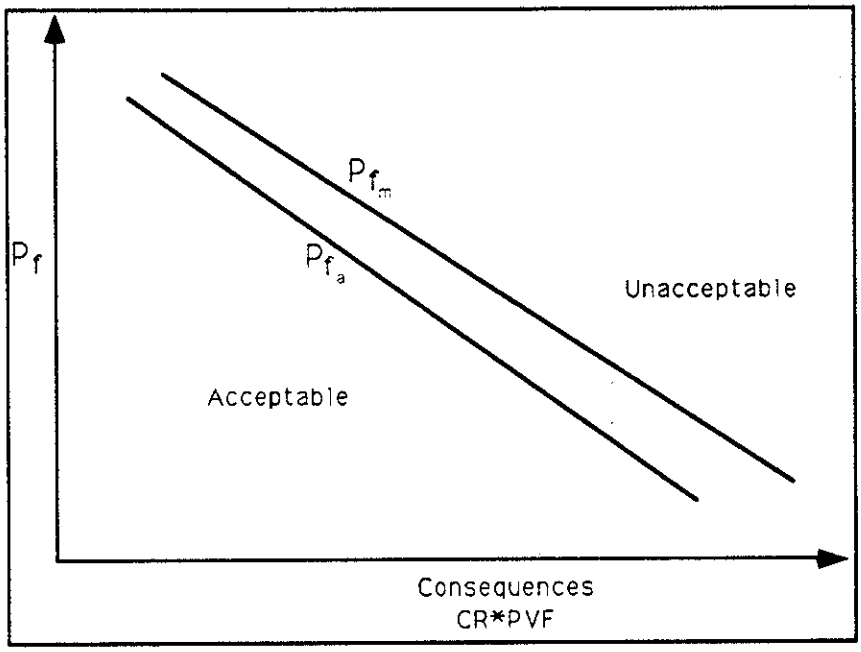


Figure 6.6 - Probability versus consequence curves for acceptable and marginal probabilities of failure

[1] The value CR is the cost ratio between the cost of failure (C_f) and the slope of the cost curve (C). As expressed by Bea (1990) the cost ratio is the cost needed to decrease the likelihood of failure by a factor of 10.

$$CR = \frac{C_{failure}}{C}$$

CHAPTER 7

CASE STUDY MODELS

7.1 INTRODUCTION

This chapter applies the modeling and quantification techniques described in the Chapters 4 through 6 to four case history-based evaluations to examine the impact of HOE upon operations of tankers and offshore platforms. The case studies include analysis of both post-mortems and existing operations. The primary objective of these two applications is to confirm the modeling procedure that has been developed by this research.

The two post-mortem case studies chosen are the *Exxon Valdez* and *Piper Alpha* disasters. These cases were selected due to the sufficient level of detailed of information documented for these disasters. Figure 7.1 provides flowcharts for each post-mortem. An overview of the relevant factors involved in each disaster is provided based upon preliminary studies that have identified the HOE factors contributing to the accident scenarios [Davidson, 1990; Keeble, 1991; Moore, 1993, 1994; Moore, Bea, and Roberts, 1993; National Transportation Safety Board, 1990; Paté-Cornell, 1992; Roberts and Moore, 1992; United Kingdom Department of Energy 1988a, 1988b, 1990].

For the post-mortem studies, influence diagram representations are developed for each model based upon the relevant information provided for each disaster. Influence diagram template models are constructed that capture the primary causative mechanisms for the two classes of accidents from which the disasters were representatives: (1) tanker grounding or collision (*Exxon Valdez*), and (2) production platform gas leaks during simultaneous production and maintenance (*Piper Alpha*). Similar procedures are used for development of the influence diagrams for existing operations. Expert judgment is used to structure each existing operations model.

The HESIM is used to determine risk indices for HOEs conditional upon error contributors for each post-mortem study disaster while direct expert judgments to determine the probabilities of failure type events are used for the existing operations models. HOE management alternatives are presented and evaluated to determine the relative impacts upon the risk of each operation.

7.2 TANKER COLLISION AND GROUNDING

7.2.1 The Grounding of *Exxon Valdez*

Moore, Bea, and Roberts (1993) have established the primary contributors to the grounding of *Exxon Valdez*. First the related accident EDAs are categorized in to underlying, direct, and compounding factors (see Figure 3.9). The primary contributing factors are shown in Figure 7.2 and summarized as follows:

Underlying-contributing factors

Event: *Exxon Valdez* deviates from the outbound *traffic separation scheme* (TSS) to avoid an ice floe in the outbound lane.

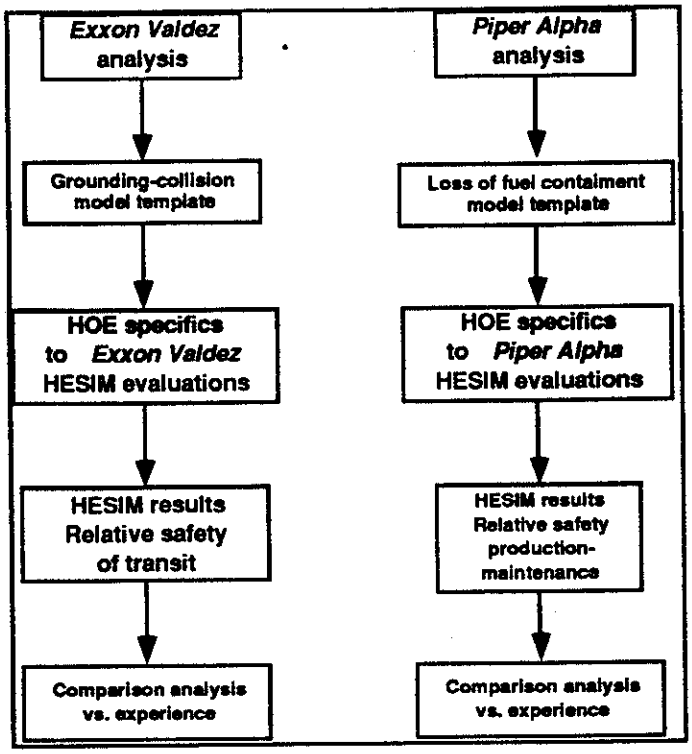


Figure 7.1 - Post-mortem analysis procedures

Causes: The deviation of from the TSS was not an isolated incident though was not recommended by either the operators nor the USCG. At the time of the grounding there had been a reduction of billets at the USCG Marine Safety Office in Valdez. On the night of the grounding the vessel traffic center (VTC) crew had not established *Exxon Valdez* on the radar nor kept in radio communication after the vessel departed from the Valdez Narrows. As the vessel deviated from the lane it was placed on automatic pilot (it is questionable as to whether the auto pilot was on until just before the grounding).

The master left the bridge leaving only the third mate in command which is in violation of Exxon Shipping operating policy. At the time of the grounding, Exxon was in the process of determining how to reduce the crew sizes aboard the vessels even though crews frequently are excessively fatigued and overworked. The chief mate was too tired to take his watch at 12 midnight since he had spent the day coordinating the loading of the vessel at the Alyeska terminal. The company had conducted no studies on the human effects of reducing crew sizes.
Conditions: Ice floe conditions in the outbound lane of the TSS was a precursor to the decision to deviate from the TSS.

Direct factors
Event: The vessel does not return to the TSS and grounds on Bligh Reef.
Causes: The USCG had problems with the radar system in Prince William Sound at the time of the grounding. It is questionable as to whether the *vessel traffic system* (VTS) personnel could properly monitor the *Exxon Valdez* on the radar. Though no radar communication may have been possible, vessel and VTS personnel had not kept in radio communication to determine the track of *Exxon Valdez*.

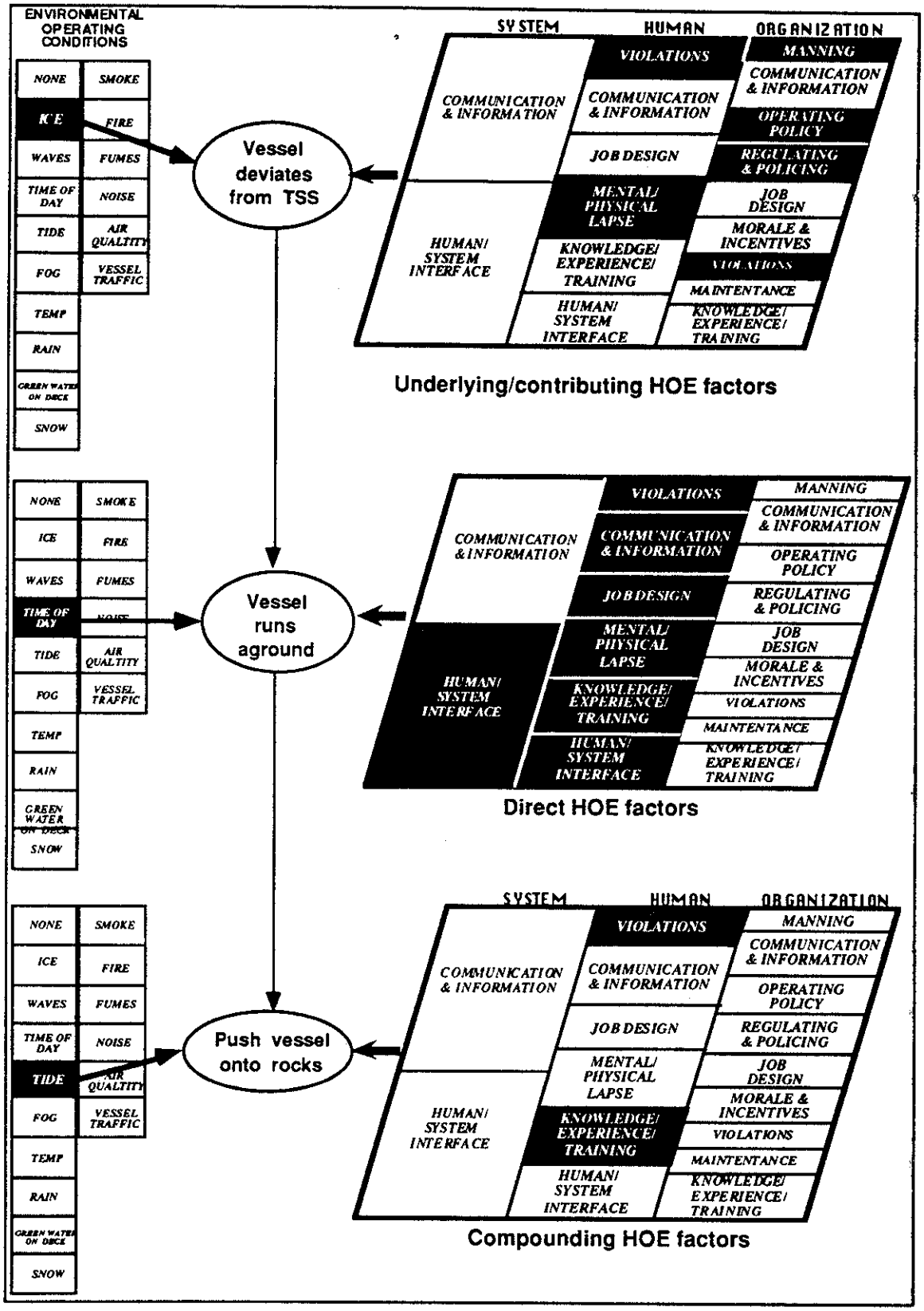


Figure 7.2 - HOE influences on the events surrounding the grounding of *Exxon Valdez*

- The third mate was unable to determine the location of the vessel just before the grounding. His lack of knowledge, training, and experience under these operating conditions had made it difficult to make proper navigation decisions.
  Conditions: The time of day was approximately midnight at or about the time of a change of watch on the bridge.

Compounding factors
Event: Captain Joseph Hazelwood, the master of *Exxon Valdez*, attempts to lodge or dislodge the vessel from Bligh Reef resulting in the compounded loss of cargo.

Cause: Captain Hazelwood may have attempted to push the vessel onto the reef to keep the vessel from capsizing. This may have been in violation of laws limiting the discharge of cargo into the water.

Conditions: At the time of the grounding the tide was dropping. This may have led to the decision to stabilize the vessel on the rocks to prevent capsizing.

7.2.2 Preliminary Influence Diagram Representation

The model incorporates critical factors both aboard *Exxon Valdez* and at the vessel traffic center (VTC) in Valdez. The underlying-contributing event is the deviation of the vessel from the traffic separation scheme (TSS). The grounding of the vessel is the direct-initiating event and the attempt to dislodge the vessel from the rocks is the subsequent compounding event that led to the additional loss of cargo. Figure 7.3 diagrams the influences between error solicitors (EDAs) leading to the grounding.

Intermediate EDAs are related to the primary events and directly influence the grounding events. Conscience actions and decisions were made by the master to: (1) deviate from the TSS, (2) depart from the bridge during transit, and (3) place the tanker on auto pilot and "load up" program. Each of these actions and decisions are represented as decision nodes.

The direct influences of HOE and environmental causes on primary and intermediate EDAs are shown in the final representation in Figure 7.4. The grounding model forms a basis from which the influence diagram template is developed.

7.2.3 Influence Diagram Template of Vessel Groundings and Collisions

Once a vessel deviates from a specific TSS within navigable waters, potential hazards (vessel traffic, reefs, currents, etc.) can greatly increase the risk of transit. An underlying factor in the events leading to the grounding of *Exxon Valdez* was the deviation of the vessel from the TSS. In analyses of tanker groundings and collisions, the following general questions are addressed in developing the influence diagram template models.

(1) Did the vessel deviate from a previously established traffic scheme? If so, was it a conscience decision to do so? It is assumed in the model that conscience decisions were made to deviate from the scheme and the deviation was not inadvertent.
(2) Was the path and location of the vessel being properly monitored? Monitoring can be performed either from an internal source (vessel crew) or external source (vessel traffic center). The monitoring of the vessel was directly related to whether a grounding or collision would occur.

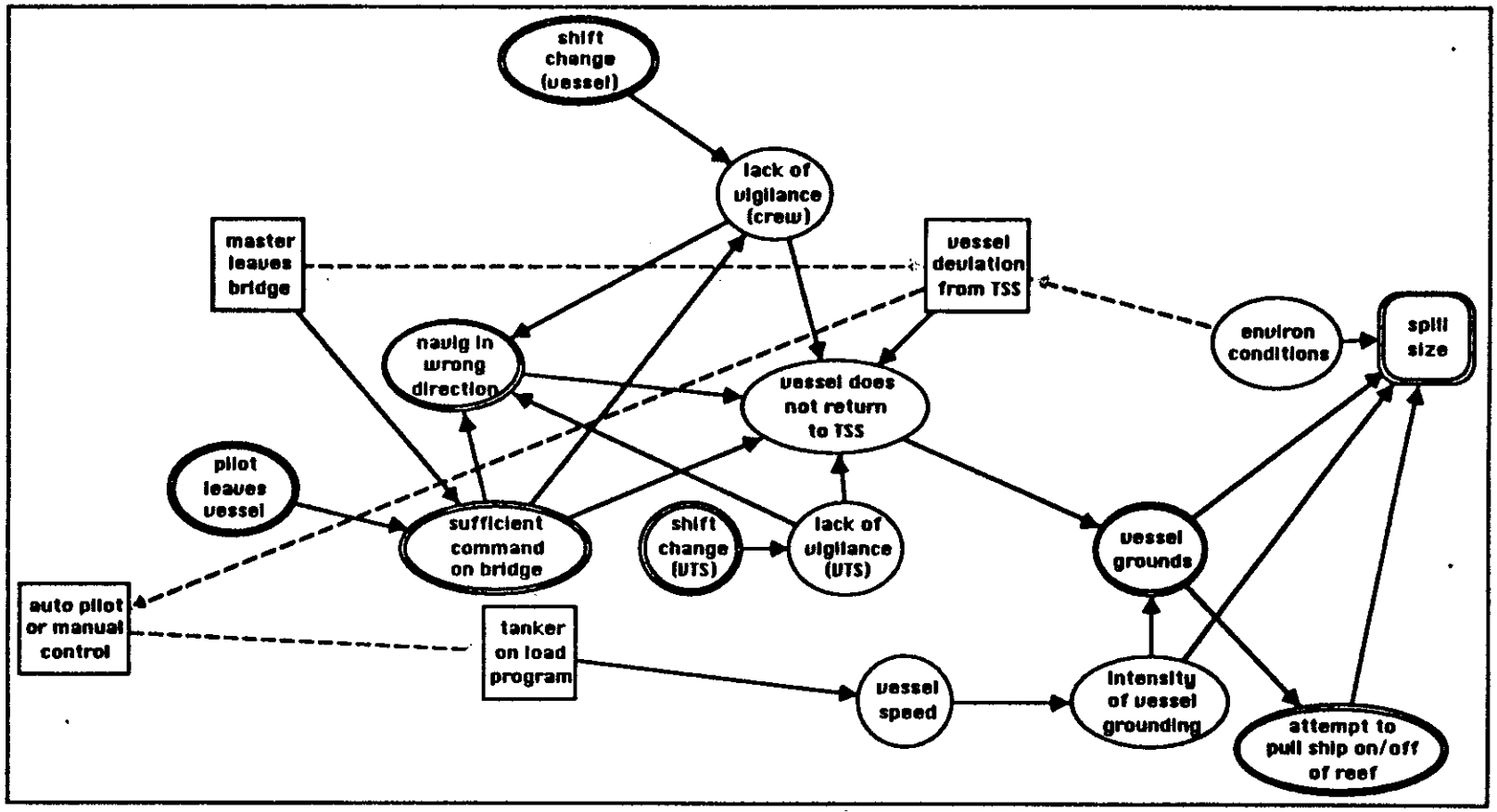


Figure 7.3 - Influence of events, decisions, and actions leading to the grounding of *Exxon Valdez*

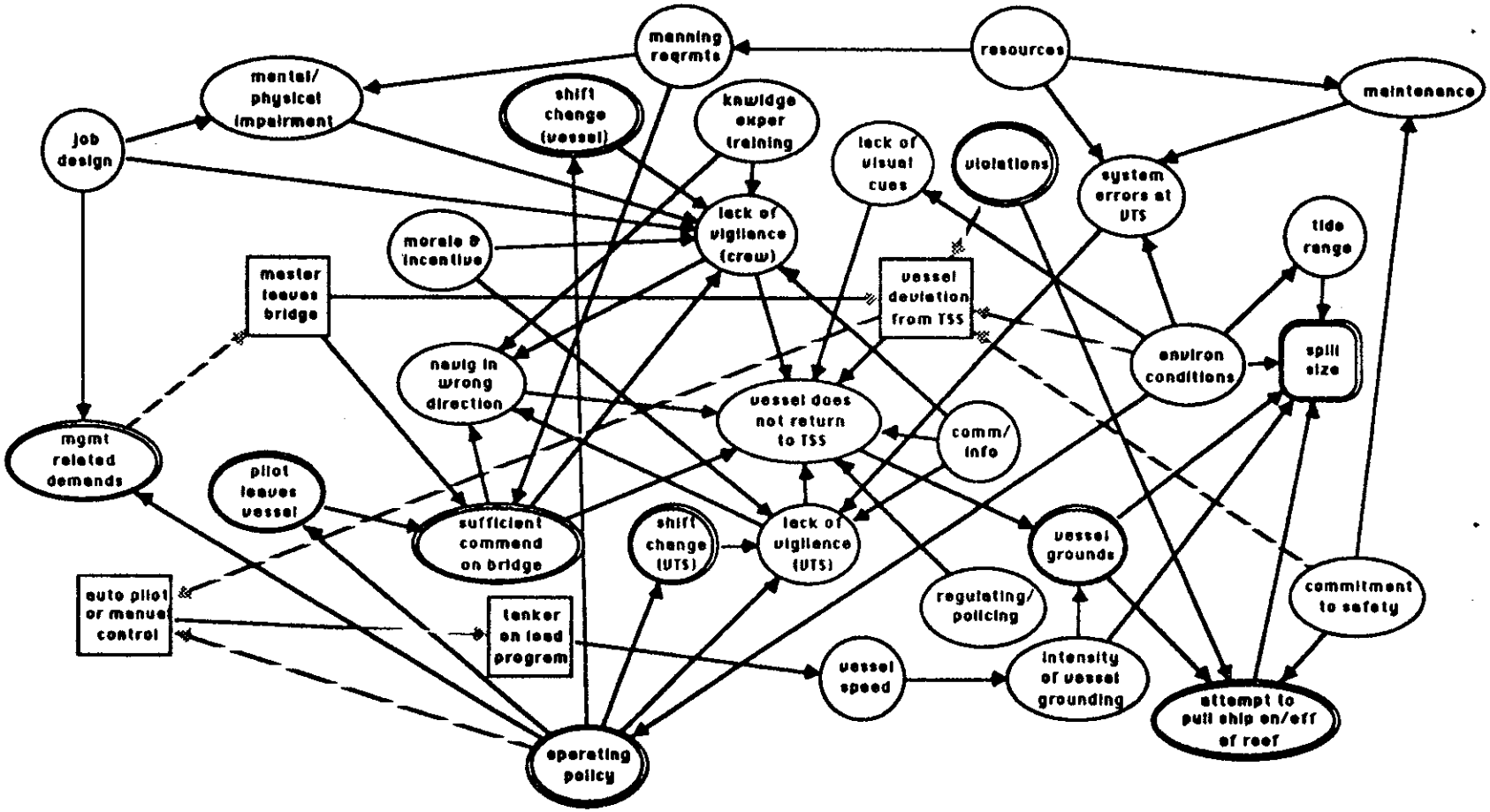


Figure 7.4: Influence diagram representation of contributing factors leading to the grounding of the tankship *Exxon Valdez*

(3) Were environmental factors (ice in the lane, waves, tide, etc.) involved in the decision to deviate from the TSS? Was vessel traffic a factor in any decision to deviate from the traffic scheme?

(4) Are ship system factors involved in the grounding of the vessel? For example, the vessel may lose power, steering, or navigation capabilities? (This issue has been of particular concern in such tanker groundings as the *Amoco Cadiz* and the *Braer*.)

(5) Were HOE's involved in the decision to deviate from the TSS and/or monitoring of vessel path? In the case of *Exxon Valdez*, a conscious decision was made to deviate from the TSS and the errors occurred after the deviation.

The influence diagram template shown in Figure 7.5 is representative of the primary causative mechanisms for a vessel grounding or collision event. The grounding of *Exxon Valdez* falls within this general class of accidents. The primary contributors are described below and the variables are shown in Table 7.1.

(1) *Environmental conditions*. The environmental operating conditions are described as a state variable since the conditions will vary from time of day to season.

(2) *Human errors*. Human errors are affected by the environmental operating conditions, the deviation from the traffic lane (non-routine) and vessel traffic (stress and non-routine). These are described as a probabilistic variable.

(3) *Deviates traffic separation scheme*. The vessel may deviate the traffic separation scheme as a result of environmental factors or vessel traffic. The deviation is represented as a probabilistic variable.

(4) *Vessel traffic*. Vessel traffic will be variable dependent upon the location and inherent variability in shipping throughput. Vessel traffic is represented as a probabilistic variable to accommodate these contributing factors.

(5) *Monitor vessel path*: Monitoring of vessel path and location is affected by deviation from the TSS and human errors. Vessel paths are assumed to be monitored if deviation occurs to prevent a grounding or collision event.

(6) *Vessel operation system failure*. Vessel operating system failure is included to account for possible loss of systems critical to the safe operation of the vessel. This includes navigational devices, power plant, or any other critical operating system. The failure of these systems are variable and are represented as a probabilistic node.

(7) *Grounding-collisions*. Groundings or collisions are directly affected by vessel traffic, TSS deviation and monitoring of vessel path, and operational system failure. The failure event is considered uncertain (probabilistic) upon the contributing factors.

(8) *Spill*[4] The possibility of a spill is conditional upon the grounding or collision of the vessel and its speed at the time of the casualty event.

---

[4] The spill, vessel speed, and spill cost nodes have been separated from the remainder of the diagram as a result of value and non-value inputs for each node in the model that lead to unrealistic coefficients of variations for the model. This is a difficulty within the *InDia*™ modeling program. These nodes are used

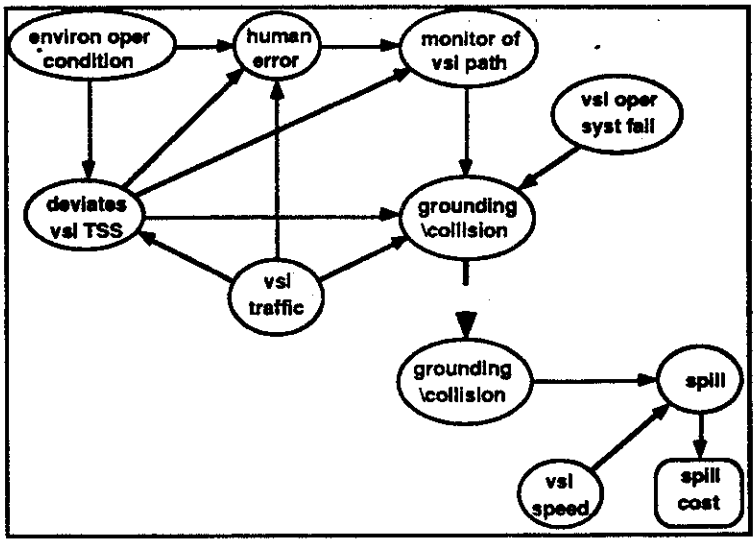


Figure 7.5 - Influence diagram model of contributing factors for tanker grounding-collision

Table 7.1 - Outcomes within each node of vessel grounding-collision influence diagram

vessel speed	**human errors**	**environ oper condition**
5 kts	*none*	*none*
10 kts	*violations*	*lane obstrct*
	comm-info	*waves*
vessel traffic	*job design*	*wind*
light	*mntl-phys lapse*	*tide*
heavy	*knwl-expr-trng*	
	hum-syst intrfc	**vessel deviates TSS**
vsl oper syst fail		*no TSS dev*
operat	**grounding-collision**	*TSS dev*
fail	*none*	
	grounding	**monitor of vessel path**
	collision	*monitor*
		no monitor

(9) *Vessel speed*[4] The vessel speed will have a direct effect upon the outflow of oil upon the grounding or collision event.

(10) *Spill cost*[4] The cost of the spill is represented as a value node to be evaluated at the end of the diagram.

7.2.4 Evaluating the Grounding-Collision Model - Reexamining the *Exxon Valdez*

The intent of this section is to determine, using the HESIM, a quantitative risks assessment of the impact of the HOE related factors to the grounding of *Exxon Valdez*. The specifics

---

in the event that reasonable probabilistic assessments are available to derive expected value and variance of the spill sizes. Though they are not directly addressed in this section (see Appendix 4).

of the disaster are used to determine the relative impact of the organizational, human factor, system, task, and environmental factors upon human errors related to the disaster. The quantitative measurements for human error and non-human error related factors are then input into the grounding-collision influence diagram model and the overall risk index of grounding-collision is assessed. The grounding-collision risk index can be compared to the grounding-collision failure probability for confirmation with the production-maintenance model probabilities and safety indices in Section 7.4.

7.2.4.1 Non-HOE related factors

In evaluating the influence diagram shown in Figure 7.5 the intent is to calculate the risk index for the grounding. Table 7.2 provides the probabilities for environmental related factors for Prince William Sound. Lane obstructions, in the case of *Exxon Valdez*, is the ice floes crossing the outbound and inbound TSSs. Prince William Sound transits approximately three tankers per day on average with a number of other vessels such as fishing boats, and an occasional container or cruise ship. The probabilities for traffic are reflected in the probability values for vessel traffic. A vessel operating system failure is presumed to be only 1 out of 500 transits (p=.002).

Table 7.2 - Nominal probabilities of operating conditions and vessel traffic for tanker transits

Environmental operating conditions:	Probability
none	.650
lane obstruction	.150
waves	.050
wind	.070
tide	.080
Vessel traffic	
light	.85
heavy	.15

7.2.4.2 HOE related factors

For the template model in Figure 7.5, human errors are conditional upon three primary contributing factors for this operation: (1) vessel traffic, (2) vessel deviation from the TSS (deviates course), (3) and the environmental operating conditions. Vessel groundings and collisions are directly dependent upon vessel path monitoring, deviation from the TSS, vessel system failure. It is assumed if the vessel path is properly monitored, human intervention is assumed to prevent a vessel grounding or collision. Each of these factors are explicitly represented in the influence diagram template shown in Figure 7.5.

As a result of no existing database documenting near collisions or groundings and related human errors, a small sample database of near grounding-collisions compiled for a 12 year period is used (10 records). Approximately 860 tanker transits per year are observed around or relative to the Prince William Sound area [National Research Council, 1991; National Transportation Safety Board, 1990]. Over a 12 year period, this accounts for 10,320 recorded transits. During certain time periods, a large number of vessel deviations from the TSS had been documented [National Transportation Safety Board, 1990]. However, no data has been collected as to particular human errors that may have increased the risks of groundings or collisions.

7.2.4.2.1 Specifics of Exxon Shipping and *Exxon Valdez*-HESIM analysis

Top Level Management

The effects of the Exxon Shipping Company upon the crew of *Exxon Valdez* has been documented as being a strong contributor to the grounding of the vessel [Davidson; 1990; Keeble, 1991; Moore, 1994; Moore, Bea, and Roberts, 1993]. The TLM weighting factors are summarized in Table 7.3. The two most heavily weighted factors for TLM impacts on human errors at the operator level are the overall commitment to safety, and the competence of operators at the front-line level. A lack of overall commitment to safety is observed since Exxon Shipping Company had allowed the master to not be present on the bridge of *Exxon Valdez* during the transit through Prince William Sound. Though it was against Exxon Shipping Company policy that the master not be present on the bridge, there were few checks and balances within the safety management system to ensure compliance. Cognizance of crew related problems was in issue in that though Exxon Shipping

Table 7.3 - Safety index criteria for vessel deviations leading to grounding of the *Exxon Valdez*

Total number of recorded transits: 10,320 records
Number of "deviate course" records: 7 records

TLM factors	TLM weight factors
overall commitment to safety	50.0%
commit to long term safety goals	10.0%
cognizance	12.5%
competence	20.0%
resources	7.5%
minimum TLM safety index	0.10
MOE factors	**Maximum degree of effect (% increase of effect)**
knowledge-training-experience	2.00 (100%)
maintenance	1.50 (50%)
violations	3.00 (200%)
morale-incentive	1.50 (50%)
job design	1.30 (30%)
regulating-policing	2.00 (100%)
operating policy	2.00 (100%)
communication-information	1.50 (50%)
manning	1.60 (60%)
Other factors	**Maximum degree of effect (% increase of effect)**
stress	2.00 (100%)
routineness	1.75 (75%)
system	1.20 (20%)
task	1.30 (30%)
environmental (external)	1.50 (50%)
environmental (internal)	1.00 (0%)

Company was aware of Captain Hazelwood's problems with alcohol, they allowed him to be on active duty while not keeping abreast of his drinking problem. The weighting of other TLM factors were spread relatively even amongst the remaining factors.

MOEs and Affects on Front Line Operator Errors

Mid-level or front-line management errors (MOEs) apply to the officers aboard the *Exxon Valdez*. Decisions and actions by the vessel's operators led to the casualty of which they were also the responsible front-line operators. The knowledge, training, and experience of the crew were sufficient aboard the vessel, although at the time of the disaster, the third mate was the only officer on watch and his experiences were limited when dealing with problems that were not necessarily routine. For tankship operations, a lack of knowledge, training, and experience can increase the risk by 100%. Aboard the *Exxon Valdez*, maintenance was not a particular contributing factor. Though maintenance of the VTS system was a particular contributor to the accident scenario. The risk is considered to be increased by 50% as a result of the effects of maintenance.

Violations are presumed to be the greatest management related contributor. Both violations of company and regulatory policy by the crew were observed for the disaster. The factors of having the vessel on automatic pilot during transit, insufficient licensed personnel on the bridge, alcohol abuse, and deviating the TSS were all major violations that led to the accident scenario. These factors increase the risks of violation contributions by 200%. Morale and incentives of the master of *Exxon Valdez* were insufficient. The moral of the officers, primarily the master, was at a low as a result of Exxon Shipping Company's policies of dismissals of tanker masters over the years prior to the disaster. Crew sizes had also been shrinking. This led to a feeling of limited job security of the master and crew. The effects of morale and incentives are presumed to increase the risk by 50%.

Regulating and policing and operating policies of both Exxon Shipping Company and regulatory bodies (federal and state) were primary contributors to the accident scenario. As mentioned above, little effort was made by the organization or regulatory bodies to ensure alcohol abuses were not going on aboard the vessel. Operating policies regarding departing the TSS while ensuring safe transits were of concern. No additional safety precautions were in place to ensure safety when leaving the TSS. The regulating, policing, and operating policies are presumed to each increase the risk by 100% due to the strong influence of these factors on operational safety.

Communication and information within the organization were of concern particularly with regard to keeping abreast of Captain Hazelwood's alcoholism problem. These are presumed to only have marginal effect on the risk, in this case, of only 50%. The issue of manning has been debated as to the impact upon the accident. *Exxon Valdez* did have sufficient personnel beyond the number (25 personnel) required by the USCG. Although, the chief mate had been working on cargo loading duties and was unable to maintain sufficient deck duties when the vessel left the Alyeska terminal. Manning factors are presumed to affect the risk of errors by 60%.

Other related factors

There were also contributions of task, system, and human factors related to errors when the vessel deviated course. Records indicate that there had been a number of course deviations to avoid ice (lane obstructions) since 1981 [National Transportation Safety Board, 1990]. This leads to a smaller valuation of the additional effects of routineness at only 75%. However, since the third mate was the lone officer on the bridge, the stress level is presumed to be a strong contributor by being a strong risk contributor at 100%.

Aboard *Exxon Valdez*, the system and task related contributions are not presumed to be major contributors as a result of the sufficient technology to perform the duties at hand. Thus the only contributions to risk for these two factors are 20% and 30% respectfully. The effects of external environmental factors for the accident scenario are presumed to be the ice floe in the outbound TSS, time of day (midnight), and the snow and sleet. No internal environmental factors were contributors to the accident.

Table 7.4 shows Exxon Shipping's TLM abilities to sufficiently address each MOE and the MOE related inputs for the transit of *Exxon Valdez* in Prince William Sound before the grounding where *sufficient* (Suff) or *insufficient* (Insuff) inputs for each TLM and MOE combination are summarized. The ratings of each MOE for the transit of the vessel are also included.

Table 7.4 - TLM-MOE relations for grounding of *Exxon Valdez* and ratings of MOE factors

	MOE_1	MOE_2	MOE_3	MOE_4	MOE_5	MOE_6	MOE_7	MOE_8	MOE_9
TLM_1	Suff	Suff	Insuff	Insuff	Suff	Insuff	Insuff	Suff	Suff
TLM_2	Suff	Suff	Suff	Suff	Suff	Insuff	Insuff	Suff	Insuff
TLM_3	Suff	Suff	Insuff	Insuff	Insuff	Insuff	Insuff	Insuff	Suff
TLM_4	Suff	Suff	Insuff	Insuff	Suff	Insuff	Insuff	Insuff	Insuff
TLM_5	Suff	Suff	Suff	Insuff	Suff	Suff	Suff	Suff	Suff
MOE rating	Fair	Fair	Poor	Fair	Fair	Poor	Poor	Poor	Fair

Table 7.5 shows the impact of the system, task, and human factors for the individuals responsible for the transit of the *Exxon Valdez*. Low system complexities are observed for the vessel, however system related factors at the VTS hampered the monitoring of the vessel path and thus overall system complexities were moderate. Task complexities were high given the limited experiences of the third mate to direct the ship under these conditions. The stress related to this task as a result of the unfamiliarity of the third mate to his assigned bridge watch was considered high. Though the routineness of the operation was moderate as a result of these deviations from the TSS not being altogether uncommon.

Table 7.5 shows the impact of the system, task, and human factors for the individuals responsible for the transit of the *Exxon Valdez*. Low system complexities are observed for the vessel, however system related factors at the VTS hampered the monitoring of the vessel path and thus overall system complexities were moderate. Task complexities were high given the limited experiences of the third mate to direct the ship under these conditions. The stress related to this task as a result of the unfamiliarity of the third mate to his assigned bridge watch was considered high. Though the routineness of the operation was moderate as a result of these deviations from the TSS not being altogether uncommon.

Using a factoring constant $k_{ij}=10^3$, the human error safety indices for the vessel deviating the TSS are generated and shown in Table 7.6. Monitoring errors are also observed for course deviations as a result of human errors and are also summarized in Table 7.6.

Table 7.5 - HESIM factors for *Exxon Valdez* transit in Prince William Sound

HESIM Factor	
system complexity	moderate
task complexity	high
stress	high
routineness	moderate
environmental (ext)	high
environmental (int)	low

Table 7.6 - Conditional risk indices of human errors for deviating course for grounding-collision model for *Exxon Valdez*

Human Errors	Risk Index (1-Safety Index)
human system interface	2.22×10^{-3}
knowledge-training-expr	2.22×10^{-3}
mental physical lapse	2.23×10^{-3}
violations	2.22×10^{-3}
job design	2.22×10^{-3}
communication-information	2.14×10^{-3}

Human Errors	no deviation of course RI[insufficient monitor|human error]	deviation of course RI[insufficient monitor|human error]
none	.0005	.005
human system interface	.0500	.100
knowledge-training-expr	.0250	.050
mental physical lapse	.0250	.050
violations	.0750	.150
job design	.0125	.025
communication-information	.0750	.150

7.2.4.3 Safety index evaluation for *Exxon Valdez*

Table 7.7 summarizes the risk index evaluation for the grounding of *Exxon Valdez* and the related human error safety indices for the grounding. The safety indices of human errors conditional upon each of these disaster types are also shown. The primary human error contributors to groundings and collisions are observed to be violations and communication-information errors. Further analysis of addressing the impacts of human errors is further discussed in Appendix 7.

Table 7.7 - Annual risk indices of groundings and collisions and the associated human errors for each event

Event	RI[grounding-collision]	
collision	5.89×10^{-4}	
grounding	1.67×10^{-3}	
Human Error	**RI[human error|collision]**	**RI[human error|grounding]**
human system interface	2.52×10^{-3}	3.54×10^{-3}
knowledge-training-exper	1.59×10^{-3}	2.26×10^{-3}
mental physical lapse	1.60×10^{-3}	2.27×10^{-3}
violations	3.45×10^{-3}	4.82×10^{-3}
job design	1.12×10^{-3}	1.61×10^{-3}
communication-information	3.32×10^{-3}	4.63×10^{-3}

7.2.5 Evaluating Alternatives for the Grounding and Collision Model -An Example

Organizational factors

The following example is a description of a well operated tanker fleet with a high commitment to safety and resources made available for safe operation. A regional organization, Company A, has a reputation of safety that has been commended throughout the industry. They have kept detailed records of operational problems that have arisen over the last 10 years. In the area of groundings and collisions, they have recorded 10 records of near misses over the last 15 years with no contact with moving or stationary bodies (collisions or groundings).

Company A pays particular attention to operating problems and conditions at the operator level by screening tankship crews and operating management. Mid-level management primarily consists of former tankship mates and officers who are well aware of problems at the operator level. These management personnel are in direct communication with top-level management personnel. When problems do occur at the operator level, they are reviewed within a reasonable time period. Personnel throughout the organization are well motivated to communicate areas that are in need of improvement with both operational issues as well as maintenance issues. Severe violations of company policy lead subjects to dismissal while minor violations normally result in minor reprimand though the violations are recorded.

Human factors

Company A operates 5 very large crude carrier (VLCC) tankers between the U.S. west Coast and Valdez, Alaska. The tankers are U.S. flag ships with U.S. crews. The officers aboard each vessel are well trained, experienced, and knowledgeable with an average of over 60 years of experience between them. However, deck crews have seamen with little or no experience as a result of limited U.S. merchant marines going to sea. Though Company A is aware of the experience problems, average years experience of the seamen is 2.5 years and an average age of 22 years. However, Company A has compensated by crewing the vessels with an average of 27 total personnel, exceeding U.S. Coast Guard manning requirements. There is a commitment by the organization to compensate for the inexperienced deck crews by maintaining full time boatswains to supervise the crews.

The vessels

Each of the 5 single-hull VLCC tankers are equipped with the latest bridge technology: radar, global positioning system, communication devices, etc. The oldest vessel in the fleet is 12 years old while the newest vessel is only 5 years old (all pre-OPA 90 vessels). The

organization has maintained detailed records of vessel maintenance and have fulfilled a commitment to maintaining a safe vessel fleet with regard to each vessel's structure, machinery, and operation.

7.2.5.1 Non-HOE related factors

In evaluating the influence diagram shown in Figure 7.5, the two particular values of concern are the probabilities of groundings or collisions given human errors and the expected costs of a spill. Spill size data were determined from VLCC collision and grounding models using the discretization process described in Appendix 5 [Det Norske Veritas, 1991]. The probabilities for spill sizes for a grounding or collision for a standard VLCC design are provided in Table 7.8.

Environmental operating conditions will differ between seasons and locations. Vessel traffic is dependent upon location of the study. Sensitivity analysis may be performed on these variables to determine the impact of the variations in the conditions. For the model the nominal values for environmental operating conditions and vessel traffic are shown in Table 7.9.

A vessel operating system failure is presumed to be only 1 out of 500 transits (p=.002). Vessel operating speeds in the areas of vessel traffic are presumed to be 5 knots 70% of the time and 30% of the transits are at 10 knots. Spill costs are estimated at mean value of $30,000.[5]

Given the information provided above concerning Company A's safety record and organizational factors, the company is assumed to be a proactive organization with few operational problems. As a result of the small number of near collisions-groundings, Company A has compiled few records over 15 years (10 records). All records were recovered from the collision-grounding database and used in the analysis and there is a greater need to use judgment in quantifying HOEs and their contributing factors. Using the HESIM, the following information in Table 7.10 was used to derive the safety indices for human errors conditional upon organizational, human factors, system, and environmental factors.

7.2.5.2 HOE related factors

For the template model in Figure 7.5, human errors are conditional upon three primary contributing factors for this operation: (1) vessel traffic, (2) vessel deviation from the TSS (deviates from course), (3) and environmental operating conditions. Vessel groundings and collisions are directly dependent upon vessel path monitoring, deviation from the TSS, and vessel system failure. It is assumed that if the vessel path is properly monitored, human intervention will prevent a vessel collision or grounding. Each of these factors are explicitly represented in the influence diagram template shown in Figure 7.5.

Based upon the conditions presented in Table 7.10, the safety indices for each human error was determined. External environmental conditions were determined for "low", "moderate", and "severe conditions". Environmental factors include low routineness and system factors and moderate stress and task factors related to the course deviation problem. Environmental factors include low task and system factors and moderate stress and routineness factors related to the monitoring problem. The risk indices for each human error conditional upon the error inducing factors presented above are shown below for

---

[5] The cost of the *Exxon Valdez* spill was approximately $30,000 per barrel spilled. Many contributing factors affect the cost per barrel; such as spill location, size, type of oil (product or crude), cleanup procedures, legal fees, etc. Cost estimates should be modified to incorporate those factors that best fit the specifics of that location.

vessel course deviation in Table 7.11. The factoring constant $k_{ij}=10^3$ for all human errors i and organizational errors j. Table 7.12 shows the judgment based conditional probabilities of proper monitoring of the vessels position relevant to whether the vessel deviated the TSS.

Table 7.8 - Conservative discharge estimates for tanker groundings and collisions for fully loaded VLCC single-hull design[6]

Casualty event	Probability	Spill size in barrels (bbls)
Collision	.22	12,750
	.28	25,500
	.25	38,250
	.20	59,497
	.05	178,000
Grounding (5 kts)	.2	25,500
	.35	35,700
	.3	51,000
	.15	76,500
Grounding (10 kts)	.08	71,400
	.5	91,800
	.3	112,200
	.12	122,400

Table 7.9 - Nominal probabilities of operating conditions and vessel traffic for tanker transits

Environmental operating conditions:		probability
	none	.900
	lane obstruction	.002
	waves	.005
	wind	.010
	tide	.083
Vessel traffic		
	light	.75
	heavy	.25

6 Standard VLCC design with a 330,000 dwt capacity, 315 m long, 57.2 m breadth, 20.8 meter draft, .83 block coefficient.

Table 7.10 - Safety index criteria for grounding-collision model for Company A

Total number of recorded transits: 10,320 records
Number of "vessel deviates course" records: 10 records

TLM factors	TLM weight factors
overall commitment to safety	55%
commit to long term safety goals	15%
cognizance	10%
competence	10%
resources	10%
minimum TLM safety index	.85
MOE factors	**Maximum degree of effect (% increase of effect)**
knowledge-training-experience	2.0 (100%)
maintenance	1.2 (20%)
violations	2.0 (100%)
morale-incentive	1.1 (10%)
job design	1.3 (30%)
regulating-policing	2.0 (100%)
operating policy	2.0 (100%)
communication-information	1.7 (70%)
manning	1.9 (90%)
Other factors	**Maximum degree of effect (% increase of effect)**
stress	1.2 (20%)
routineness	1.5 (50%)
system	1.1 (10%)
task	1.3 (30%)
environmental (external)	1.5 (50%)
environmental (internal)	1.0 (0%)

Table 7.11 - Conditional risk indices of human errors for deviating course for grounding-collision model - Company A

Human Errors	Risk Index (1-Safety Index): Environmental factors -low (excluding vessel traffic)			
	Light vessel traffic		Heavy vessel traffic	
	Low task routineness	High task routineness	Low task routineness	High task routineness
human system interface	1.90×10^{-6}	2.58×10^{-6}	2.28×10^{-6}	3.37×10^{-6}
knowledge-training-expr	1.90×10^{-6}	2.58×10^{-6}	2.28×10^{-6}	3.37×10^{-6}
mental physical lapse	1.90×10^{-6}	2.58×10^{-6}	2.28×10^{-6}	3.37×10^{-6}
violations	1.90×10^{-6}	2.58×10^{-6}	2.28×10^{-6}	3.37×10^{-6}
job design	1.90×10^{-6}	2.58×10^{-6}	2.28×10^{-6}	3.37×10^{-6}
communication-information	1.90×10^{-6}	2.58×10^{-6}	2.28×10^{-6}	3.37×10^{-6}
Human Errors	Risk Index (1-Safety Index): Environmental factors -high (excluding vessel traffic)			
	Light vessel traffic		Heavy vessel traffic	
	Low task routineness	High task routineness	Low task routineness	High task routineness
human system interface	2.58×10^{-6}	2.85×10^{-6}	3.09×10^{-6}	4.22×10^{-6}
knowledge-training-expr	2.58×10^{-6}	2.85×10^{-6}	3.09×10^{-6}	4.22×10^{-6}
mental physical lapse	2.58×10^{-6}	2.85×10^{-6}	3.09×10^{-6}	4.22×10^{-6}
violations	2.58×10^{-6}	2.85×10^{-6}	3.09×10^{-6}	4.22×10^{-6}
job design	2.58×10^{-6}	2.85×10^{-6}	3.09×10^{-6}	4.22×10^{-6}
communication-information	2.58×10^{-6}	2.85×10^{-6}	3.09×10^{-6}	4.22×10^{-6}

Table 7.12 - Conditional probabilities of human errors for deviating course for grounding-collision model - Company A

Human Errors	no deviation of course P[insufficient monitoring]	deviation of course P[insufficient monitoring]
none	.005	.05
human system interface	.05	.25
knowledge-training-expr	.05	.15
mental physical lapse	.05	.15
violations	.25	.35
job design	.01	.10
communication-information	.25	.50

7.2.5.3 Evaluation of the model

Evaluating the influence diagram results in risk indices of groundings and collisions as summarized in Table 7.13.[7] Violations, communication, and information problems present the largest risk indices for this model. The expected cost of a product spill is $72,420 with a standard deviation of $26,732.[8]

Table 7.13 - Annual risk indices of groundings and collisions and the associated human errors for each event

Event	RI[grounding-collision]	
collision	2.00×10^{-4}	
grounding	1.21×10^{-4}	
Human Error	**RI[[human error|collision]**	**RI[[human error|grounding]**
human system interface	1.04×10^{-5}	6.70×10^{-6}
knowledge-training-expr	8.00×10^{-6}	6.20×10^{-6}
mental physical lapse	8.00×10^{-6}	6.20×10^{-6}
violations	2.48×10^{-5}	2.14×10^{-5}
job design	4.40×10^{-6}	3.10×10^{-6}
communication-information	2.79×10^{-5}	2.11×10^{-5}

7.2.5.4 Evaluating HOE Management Alternatives for Tanker Grounding-Collision -Tug Escorts

As described in Chapter 6 three forms of management alternatives are available to the operating system: directly addressing HOE through HOE management programs, changes in operational procedure, and development of human error tolerant systems. The HOE management alternative described is a change of operational procedure. The HOE management alternative modeled is the required tug vessel support specified by the *Oil Pollution Act of 1990* (OPA 90).

Since the grounding of *Exxon Valdez*, the most influential changes for tanker operations in U.S. territorial waters has been the *Oil Pollution Act of 1990* (OPA 90). OPA 90 addresses a wide variety of tanker operation issues and are representative of current HOE management alternatives. As an overview, Title IV of OPA 90 [Connaughton, 1990]:

(1) mandates that the Coast Guard tie into the National Driving Register to detect individuals with drunk driving convictions;

(2) increases Coast Guard authority to deny or revoke mariner licenses and documents;

---

[7] This is not directly a probability of grounding since risk indices were used as a quantitative measure of human errors. In addition, the human error indices are a measure of the error being the *primary* contributor. Other human errors may be observed in the accident sequence.

[8] This expected cost is based upon the safety index value and not the probability of failure. As discussed in Chapter 4, through time, as the safety index evaluations are updated such that one is able to calibrate the safety index with the reliability of the system, one is able to make a direct assessment as to the expected cost and standard deviation.

(3) authorizes removal of incompetent personnel;

(4) increases Coast Guard authority to deny entry of foreign vessels into the U.S. waters on the grounds of deficient manning;

(5) limit crew work hours aboard tankers to 15 hrs/day but no more than 36 hours in any 72 hour period;

(6) mandates the Coast Guard conduct studies on vessel traffic and tanker navigation;

(7) requires all new tanker builds to be double-hulled in addition to the phasing out of existing tankers beginning in 1995 and concluding in 2010; and,

(8) require the Coast Guard to designate areas where two licensed personnel are required on the vessel bridge and tug escorts are necessary.

Figure 7.6 is an influence diagram representing tug support to tank vessels for transit through navigable waters. This management alternative demonstrates a change in operational procedure that can reduce the effects of human errors at the operator level (see Chapter 6). The tug support is presumed available during most environmental conditions except for high seas (waves). In the event of a vessel system failure, tug support is assumed available to assist the vessel in addition to assisting in monitoring the vessel's position and location.

The effect of the tug support is an increase in the reliability of monitoring vessel path and a reduction of the probability of grounding-collision. It is assumed that the primary reductions in human errors at the operator level are in violations, communication and information, mental and physical lapses, knowledge, training, and experience. Tanker crews are less willing to violate transit laws when tugs are present (regulating and policing). Communication and information problems for vessel crews are reduced since the tug crews are knowledgeable of the waters being transited. The experience of the tug crews also reduces problems of knowledge, training, and experience of the tanker crews. Mental and physical lapses are less likely to occur if proper communication and information as to the vessel's location and position is being exchanged between tanker and tug crews.

It is assumed for Company A, however, that the deck officers are well trained, experienced, and knowledgeable. For Company A, the significant impact of tug support has been in the monitoring aspects of vessel transits. It is presumed that human errors in monitoring are reduced by 80% after the implementation of tug support was available and are presented in Table 7.14.

By evaluation of the tug escort influence diagram in Figure 7.6, the risk indices for groundings and collisions and risk indices of human errors conditional upon the grounding or collision are generated and presented in Table 7.15. Significant reductions in the incidence of human errors are observed as a result of the tug service. Recall that for Company A, the impact of tug escort came primarily in the monitoring aspects of the operation.

Substantial impacts upon the incidence of human errors as well as the risk of groundings has been observed. The incidence of violations as primary cause of collisions has dropped 83% and 60% for groundings. Communications-information errors have been reduced by 85% for collisions and 59% for groundings. Mental and physical lapses have been reduced by more than 85% for collisions and 59% for groundings. Initiations of accidents resulting

from human system interface errors for collisions and groundings are reduced by 73% and 67% respectively. The expected cost (risk index cost) of a product spill if tug support is available is $42,943 with a standard deviation of $14,421. This is a net expected benefit of $29,477 which equates to a 40.7% reduction in cost.

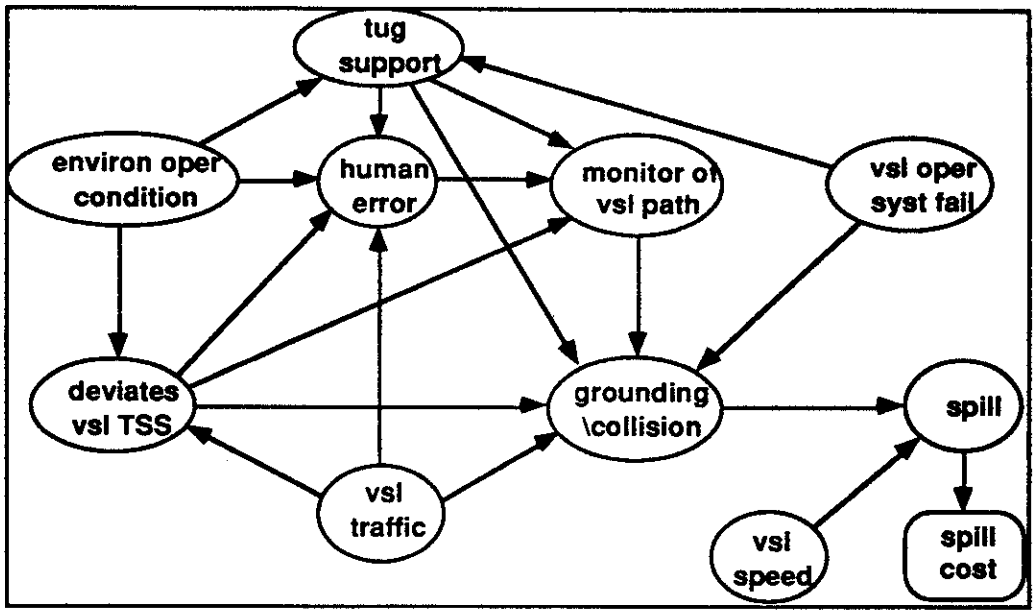


Figure 7.6 - Influence diagram model designed to model affect of tug support

Table 7.14 - Conditional probabilities of human errors for deviating course for grounding-collision model with tug support - Company A

Human Errors	no deviation of course P[insufficient monitoring]	deviation of course P[insufficient monitoring]
none	.001	.01
human system interface	.01	.05
knowledge-training-expr	.01	.03
mental physical lapse	.01	.03
violations	.05	.07
job design	.002	.02
communication-information	.05	.10

Table 7.15 - Annual risk indices of groundings and collisions and the associated human errors for each event

Event	RI[grounding-collision]	
collision	1.76×10^{-4} (12%)	
grounding	7.04×10^{-5} (42%)	
Human Error	**RI[human error|collision]**	**RI[human error|grounding]**
human system interface	2.80×10^{-6} (73%)	4.20×10^{-6} (37%)
knowledge-training-expr	2.70×10^{-6} (66%)	3.90×10^{-6} (37%)
mental physical lapse	2.70×10^{-6} (66%)	3.90×10^{-6} (37%)
violations	4.20×10^{-6} (83%)	8.50×10^{-6} (60%)
job design	2.40×10^{-6} (45%)	3.80×10^{-6} (-18%)
communication-information	4.30×10^{-6} (85%)	8.70×10^{-6} (59%)

7.3 OFFSHORE PLATFORM - SIMULTANEOUS PRODUCTION and MAINTENANCE

7.3.1 The *Piper Alpha* Disaster

Figure 7.7 provides a schematic diagram of the influence of causes and conditions upon the events surrounding the *Piper Alpha* disaster. The primary set of accident events of the *Piper Alpha* disaster and their related causes are summarized as follows [Paté-Cornell, 1992]:

Underlying-contributing factors

Event: Decision to conduct critical maintenance and produce simultaneously.

Causes: Occidental management had decided to perform simultaneous production and maintenance even though the maintenance required the shutting down of critical emergency safety systems. This displays a lack of commitment to safety by the operators who show little regard for a safe production process.

Conditions: Night crew change, wind blowing across platform in direction of quarters, production at highest possible level.

Direct factors

Event: Initial explosion in Module C resulting from a leak in condensate pump A at a blind flange assembly leads to a chain of explosions, fires, fumes, and smoke engulfing the platform in a matter of minutes.

Causes: Maintenance crews in Module C had not informed control room operators of the maintenance status of the condensate pumps. There was an improper assembly of the blind flange on condensate pump A. There was minimal warning as to the escalating conditions in Module C prior to the initial explosion. The emergency gas detection system had been partially decommissioned or was completely incapacitated.

Conditions: Initial explosions occurred at approximately midnight.

Compounding factors

Event: The death of 167 men and the total loss of the platform.

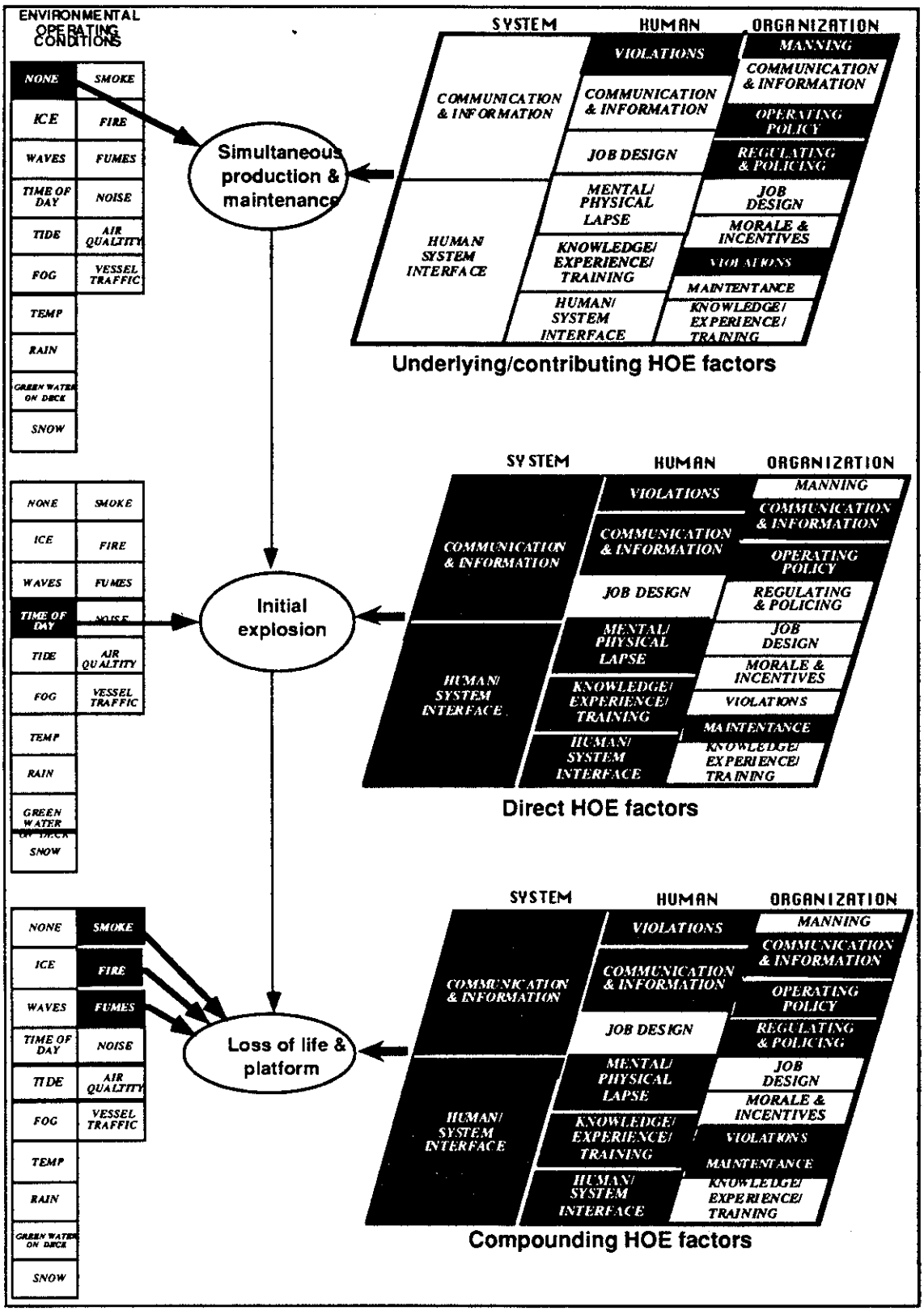


Figure 7.7 - HOE influences on the events surrounding the *Piper Alpha* disaster

Cause: The events succeeding the initial explosions and fires were compounded by the lack of available escape routes, a lack of experience, training, and knowledge of the operating personnel (only 26 men were permanently stationed on the platform at the time of the disaster). The emergency lighting, deluge, and communication systems were completely inoperable moments after the initial explosion. There were no orders given to evacuate the platform.

The *M.S .Tharos* role in controlling the fire and rescuing personnel was limited though the semi-submersible was fully equipped to handle offshore fires.

At the time of the accident, the *Claymore* and *Tartan* platforms had been piping high-pressure gas to *Piper Alpha*. The failure of the offshore installation managers of *Tartan* and *Claymore* failed to immediately shut down production operations led to further loss of life and platform. Though the platform had been cited for a number of safety violations by the Department of Energy, few changes had been implemented.

Conditions: Smoke, fire, and fumes engulf the platform making it virtually impossible for control of the fire or escape of personnel from the accommodations unit where 84 men die.

The impact of smoke, fire, and fumes also resulted in an escalation of catastrophic events. Figure 7.7 shows the impact of HOEs and environmental operating conditions on the primary accident events. The accident occurred at night immediately after a maintenance crew change. The crew change is related to the explosion-fire event. The loss of life and platform were affected by smoke, fire, and fumes at various stages as the accident progressed.

7.3.2 Preliminary Model Representation

A primary factor leading to the *Piper Alpha* disaster was the decision to produce and perform critical process maintenance simultaneously [Paté-Cornell, 1992; United Kingdom Department of Energy, 1990]. Miscommunication between control room and maintenance crews regarding the maintenance status on a condensate pump led to a gas leak. Another concern in analyzing the accident was the loss of fuel containment which led to the compounding of catastrophic events. Fuel containment was lost in Module B, Module C, helicopter fuel storage on the deck, and gas risers from the *Claymore* and *Tartan* platforms.

Figure 7.8 is an influence diagram representation of the EDAs surrounding the *Piper Alpha* disaster. It is presumed that three primary factors contributed to the accident sequence: (1) simultaneous production and maintenance, (2) initial explosion, and (3) loss of life and platform.

Intermediate EDAs are related to the primary events and directly influence the eventual outcome. Conscience decisions were made to produce (103,000 bbl/day) and conduct process critical maintenance (PSV 504 on condensate pump A in Module C) concurrently. The maintenance status of condensate pump A was not communicated between the maintenance and control room personnel (failures in permit to work system). Condensate pump A was started by control room personnel once condensate pump B had tripped. The leak at the blind flange assembly on condensate pump A led to the initial process leak.

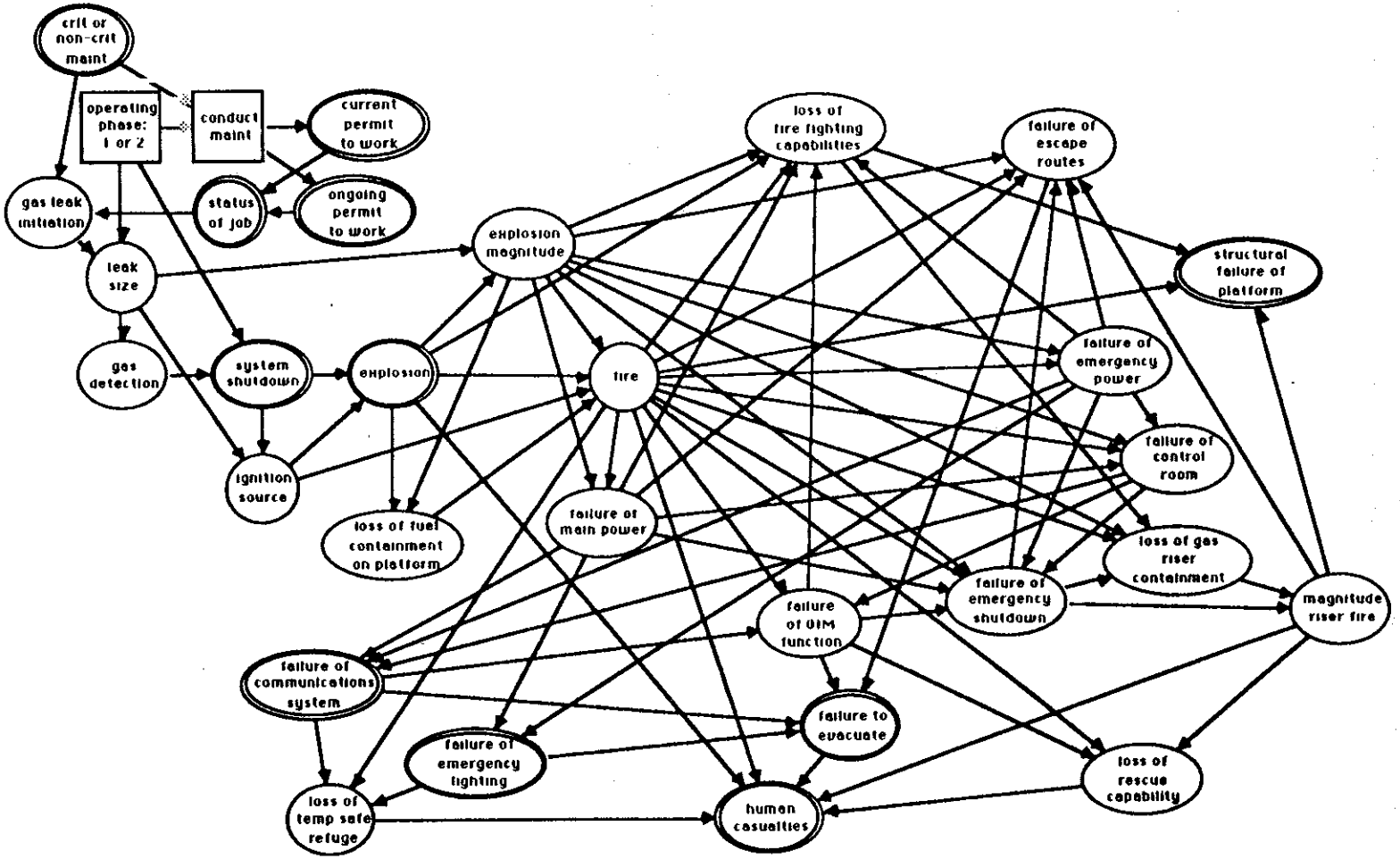


Figure 7.8: Influence diagram representation of contributing factors leading to the *Piper Alpha* disaster

Ignition of the fuel sources and the subsequent fires and explosions led to the loss of electrical power, *offshore installation manager* (OIM), control room and emergency systems. These factors led to loss of safe refuge, escape routes, rescue capabilities, and eventually a catastrophic loss of life and platform.

7.3.3 Influence Diagram Template for Simultaneous Production and Maintenance

In developing the general influence diagram model, the following issues were of particular concern in the aftermath of the disaster. These issues apply to the general class of loss of fuel containment (fires and explosions) accidents for offshore production platforms. First, was the management decision to perform simultaneous process maintenance and production. Second, was the process leak event resulting from the high production level that eventually led to the series of explosions and fires. Third, was the breach of fuel containment resulting in the exposure of additional fuel sources. The *Piper Alpha* disaster was an incident falling within this particular class of accidents. Studies prior to the *Piper Alpha* disaster have shown that 76% of all United Kingdom offshore continental shelf (UK OCS) accidents occurred during maintenance operations.

The influence diagrams shown in Figure 7.9 and Figure 7.10 demonstrate the stages of an accident starting with the decision to perform maintenance and produce simultaneously and the impact that decision has on a potential process leak leading to fire or explosion. The loss of fuel containment escalated the accident to catastrophic consequences. The primary goal is to control a further loss of fuel containment in the event of an initial explosion or fire.

The model shows the initial decision to perform simultaneous production and maintenance. The decision is directly related to process leaks, process system failures, and monitoring of the platform production systems. Organizational errors have a direct impact upon human errors at the front-line operator level. Human errors influence the process leaks (maintenance) and monitoring of the platform systems (control room). Process leaks are also influenced by process system failures (process disturbances) and the human or automated monitoring of the production operation.

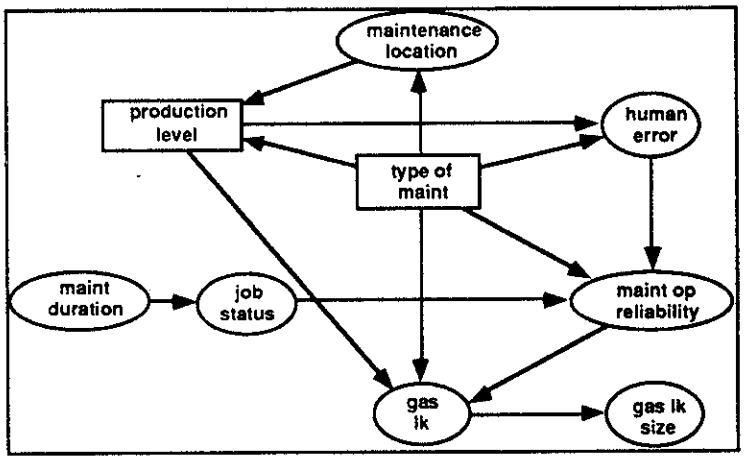


Figure 7.9 - Influence diagram of offshore production-maintenance leading to gas leak

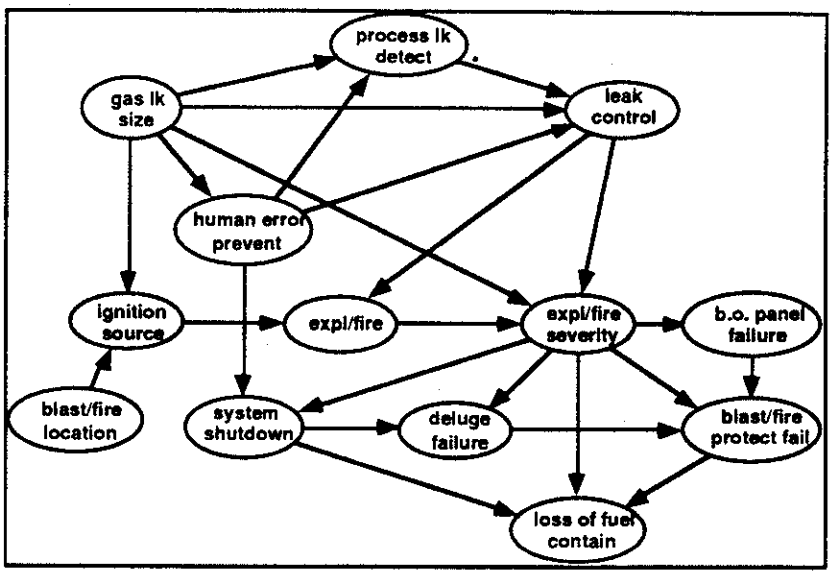


Figure 7.10 - Influence diagram of offshore gas leak leading to loss of fuel containment

Fires and explosions are influenced by process leaks, the leak location and the level at which the production and maintenance are being conducted. For example, higher production outputs during process critical maintenance have greater influence on the explosion or fire event.[9] The leak location and fire or explosion influence the loss of fuel containment aboard the platform. Fuel containment refers to any part of the platform that contains high or significant inventories of fuel sources (piping, fuel storage, production risers, etc.).

Explosions and fires are assumed not to be relevant to non-process related maintenance. For human errors, the human-system interface has a higher frequency of accident occurrences. This may be attributed to problems in the control room as a result of sub-systems being shut down for maintenance or repair and system status information may be incomplete or incorrect. This is also evident with regard to system errors. Communications-information and human system interface errors have comparatively higher frequencies of occurrence.

Figure 7.9 is an influence diagram to model crew changes and communication status of maintenance operations. This model is used to determine the effects of production levels and maintenance types upon human errors by maintenance crews. The model distinguishes between production and maintenance decisions. The maintenance location, duration, equipment, and reliability (knowledge, training, and experience of maintenance crew) are included in the model. To account for maintenance operations, job duration, job status, crew changes, communication of job status (permit to work system) directly or indirectly influence the magnitude of a process leak. To further develop the model, additional

---

[9] *Process critical maintenance* refers to maintenance on machinery and equipment directly related to production and processing hydrocarbons (separators, compressors, risers, etc.). *Non-process critical maintenance* refers to maintenance that does not directly affect the production process (e.g. accommodations, utilities areas, etc.)

modifications were made to account for the production level ("maximum", "moderate", or "none") and size of the gas leak ("small", "moderate", or "large").

Figure 7.10 is an influence diagram to account for loss of fuel containment in the event of: (1) detection and control of the process leak, (2) ignition of leak, (3) system shutdown in the event of explosion or fire, and (4) failure of power, deluge and blowout panel systems.

The primary focus of this model is to examine the influences of human factors on leak detection and control. The concern is to reduce the incidence of the explosion or fire event. The values that are generated for this model are a culmination of both safety indices and probabilities.

Detection and control of process leaks are performed both manually (operator) and automatically (system). The ability to detect and control process leaks are dependent upon the sensitivity of the detection system, experience, knowledge and training of the operating crew, and the technology available in the detection and control system.

Human performance is a function of the lead time available to respond to warnings in the system. Errors are compounded by the lack of effective early warning systems [Paté-Cornell, 1986]. As observed in Figure 7.11, if the lead time is short, there is little time allowance for corrective action before the situation reaches a critical state. On the other hand, if the system is too sensitive causing frequent false alarms, operators will eventually cease to respond to the warning signals.

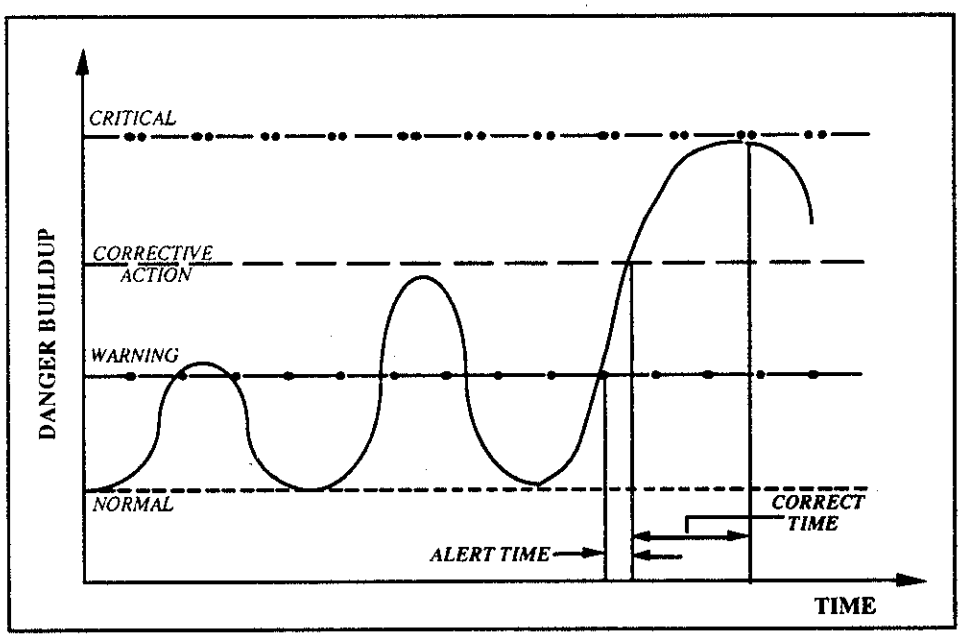


Figure 7.11 - Danger buildup function [Paté-Cornell, 1986]

As mentioned previously, process leak detection and control are dependent upon the sensitivity of the detection system and the ability of the operating crew to prevent or mitigate the effects of the leak. Better prevention and mitigation of accidents are attained through management investing in better knowledge (through training), emergency training (crisis management), experience (better screening and selection for operators), detection

(human-system interface, system communication and information), and emergency shutdown systems. Similar models discussing issues of manual and automated shutdown of systems are previously exemplified by tanker pump room fires and offshore platform module fires [Bea and Moore, 1993, 1994]. Each outcome of the model nodes are shown below in Table 7.16.

7.3.4 Evaluating the Maintenance-Production Model - Reexamination of *Piper Alpha*

The intent of this section is to determine, using the HESIM, a quantitative risks assessment of the impact of HOE related factors to the grounding of *Piper Alpha*. The specifics of the disaster are used to determine the relative impact of the organizational, human factor, system, task, and environmental factors upon the human errors related to the disaster. The quantitative measurements for human error and non-human error related factors are then input into the grounding-collision influence diagram model and the overall risk index of grounding-collision is assessed. The loss of fuel containment risk index is then compared to the loss of containment failure probability for confirmation with the grounding-collision model probabilities and safety indices.

7.3.4.1 Non-HOE Related Factors

Probabilistic assessments for each of the non-human error related nodes were determined by explosion and fire probabilities developed by Veritec for the *Piper Alpha* replacement platform, *Piper Bravo*, preliminary study [Veritas Offshore Technology Services A/S, 1989]. These failure related factors are summarized in Table 7.17.

7.3.4.2 HOE Related Factors

A sample database was used as a framework from which to perform the HESIM based analysis. As summarized in Table 7.18, there were 300 maintenance operations documented, 8 of which were observed records of casualties resulting from the simultaneous production and maintenance problems and 13 records of human errors related to threat detection and control.

Table 7.16 - Outcomes within each node of simultaneous production-maintenance and leak detection-control influence diagrams

production level	maintenance location and blast-fire location	human error and human error prevent
none	*compression*	*none*
moderate	*separation*	*hum-syst intrfc*
high	*well area*	*knwl-trn-expr*
	risers	*mntl-phys lps*
type of maint	*other*	*violation*
critical		*job dsgn*
non-critical	**maint op reliability**	*comm-info*
	reliable	
maint duration	*non-reliable*	**job status**
less than a shift		*finished*
greater than a shift	**gas lk**	*unfinished*
	yes	
gas lk sz	*no*	**process lk control**
small		*yes*
moderate	**process lk detect**	*no*
large	*yes*	
	no	**expl-fire severity**
ignition source		*small*
yes	**expl-fire**	*large*
no	*explosion*	
	fire	**deluge failure**
b.o. panel failure		*operate*
operate	**blast-fire protect fail**	*failure*
failure	*operate*	
	failure	**system shutdown**
loss of fuel contain		*operate*
no loss		*shutdown*
loss		

Table 7.17 - Non-human error tables for production-maintenance model

Maint type	Maint location				
	compression	separation	well area	risers	other
process critical	0.25	0.25	0.25	0.25	0.00
non-process critical	0.15	0.20	0.15	0.05	0.45

maintenance duration	P[maint duration]
less than a shift	0.75
greater than a shift	0.25

maintenance duration	P[finished job| maint duration]
less than a shift	1.00
greater than a shift	0.75

Production level	Maint op reliability	Type of maintenance	P[gas leak]
low	sufficient	process critical	0.0050
"	"	non-process critical	0.0005
moderate	"	process critical	0.0050
"	"	non-process critical	0.0005
high	"	process critical	0.0500
"	"	non-process critical	0.0050
low	insufficient	process critical	0.1000
"	"	non-process critical	0.0500
moderate	"	process critical	0.0050
"	"	non-process critical	0.2000
high	"	process critical	0.4000
"	"	non-process critical	0.2000

gas leak	P[leak size|gas leak]		
	Small leak	Moderate leak	Large leak
yes	0.900	0.075	0.025

Table 7.17 - Non-human error tables for production-maintenance model (cont.)

Explosion fire severity	Deluge failure	Blowout panel failure	P[blast-fire protect failure| deluge fail, b.o. panel fail, expl-fire severity]
small	operate	operate	0.020
"	"	failure	0.100
moderate	"	operate	0.05
"	"	failure	0.25
large	"	operate	0.25
"	"	failure	0.50
small	failure	operate	0.05
"	"	failure	0.15
moderate	"	operate	0.20
"	"	failure	0.30
large	"	operate	0.50
"	"	failure	0.70

System shutdown	Explosion-fire severity	P[deluge fail|system shutdown, explosion-fire severity]
shutdown	small	1.000
"	moderate	1.000
"	large	1.000
operate	small	0.005
"	moderate	0.010
"	large	0.010

explosion-fire	leak control	gas leak size	P[explosion-fire severity| expl-fire, leak control, gas leak size] Small leak	Moderate leak	Large leak
explosion	control	small	0.900	0.085	0.015
"	"	moderate	0.800	0.150	0.050
"	"	large	0.300	0.350	0.350
fire	"	small	0.900	0.005	0.095
"	"	moderate	0.800	0.150	0.050
"	"	large	0.300	0.350	0.350
explosion	no control	small	0.825	0.150	0.025
"	"	moderate	0.600	0.200	0.200
"	"	large	0.100	0.450	0.450
fire	"	small	0.825	0.150	0.025
"	"	moderate	0.600	0.200	0.200
"	"	large	0.100	0.450	0.450

Table 7.17 - Non-human error tables for production-maintenance model (cont.)

gas leak control	P[explosion or fire | ignition source, leak control] Explosion	Fire
leak control	0.05	0.05
no leak control	0.35	0.35

gas leak size	P[ignition source found| gas leak size, location] compress	separate	well area	risers	other
small	0.050	0.030	0.060	0.005	0.005
moderate	0.400	0.400	0.300	0.050	0.010
large	0.900	0.900	0.600	0.200	0.050

P[location] compress	separate	well area	risers	other
0.35	0.30	0.20	0.10	0.05

Explosion-fire severity	P[blowout panel failure| explosion-fire severity]
small	0.50
moderate	0.15
large	0.05

Explosion-fire severity	System shutdown	P[loss of fuel containment| expl-fire severity, blast-fire protect failure, syst shutdown]
small	operate	0.10
"	shutdown	0.20
moderate	operate	0.30
"	failure	0.50
large	operate	0.50
"	failure	0.70

Table 7.18- Safety index criteria for vessel deviations leading to grounding of the *Exxon Valdez*

Total number of recorded maint-production ops: 115 records
Number of "threat detection and control" records: 13 records
Number of "simul prod-maint" records: 8 records

TLM factors	TLM weight factors
overall commitment to safety	40.0%
commit to long term safety goals	15.0%
cognizance	20.0%
competence	20.0%
resources	5.0%
minimum TLM safety index	0.01
MOE factors	**Maximum degree of effect (% increase of effect)**
knowledge-training-experience	3.00 (200%)
maintenance	2.00 (100%)
violations	2.50 (150%)
morale-incentive	1.75 (75%)
job design	1.50 (50%)
regulating-policing	2.00 (100%)
operating policy	3.00 (200%)
communication-information	2.00 (100%)
manning	1.75 (75%)
Other factors	**Maximum degree of effect (% increase of effect)**
stress	1.50 (50%)
routineness	3.00 (200%)
system	1.75 (75%)
task	1.50 (50%)
environmental (external)	1.25 (25%)
environmental (internal)	1.00 (0%)

7.3.4.2.1 Specifics of Occidental Petroleum Company and *Piper Alpha*-HESIM analysis

Top Level Management

The effects of the Occidental Petroleum Company upon the operations of *Piper Alpha* have been documented as being strong contributors to the catastrophic fires and explosions that occurred on the platform [United Kingdom Department of Energy, 1990; Paté-Cornell, 1992]. Table 7.18 summarizes the impacts of TLM factors on the operations of *Piper Alpha* at the time of the disaster. Overall commitment to safety was a major contributing factor to the disaster. The dangerously high level of production and the disabling of safety systems were a direct sign of the limited commitment to safety of Occidental Petroleum Company's management to assure safety. Occidental had not properly assessed the impacts of upgrading the production system while not properly accounting for the increased risks of additional explosion and fire [Paté-Cornell, 1992]. Further minor upgrades to the system to increase production through the years also led to increased risks that were not

foreseen. This is the result of limited cognizance and competence by TLM in ensuring the long term safety goals for the system. The largest TLM related weight has been placed upon the overall commitment to safety at 40% and cognizance and competence have been weighted at 20% each.

MOEs and Affects on Front Line Operator Errors

The effects of mid-level and front-line management errors are also summarized in Table 7.18. During operations such as simultaneous production and process critical maintenance, knowledge, training and experience were critical to the safety of the system. The OIM's experiences should lead to safer decision making for the complex process. Thus the impact of knowledge, training, and experience of mid-level management is critical. Therefore, thus the risk of this factor is presumed to affect the system by 200%.

Maintenance related errors by management are also critical for production process critical systems. The permit to work system must be properly controlled and maintained to ensure both sufficient and safe work practices. Maintenance errors by mid-level and front-line operators are presumed to affect the system by increasing the risk by 100%. The effects of violations critically hampered the crew of *Piper Alpha* from ensuring safe operations. Pressures of the production schedule led to cutting corners by front-line managers without ensuring that the safety system was properly operating and maintained (deluge, alarm, and emergency shutdown systems). Given the critical nature of major violations in operations such as an inadequate permit to work system and shutdown of emergency systems during workovers, violations are presumed to increase the risk to the system by 150%.

Critical factors of job design affected the proper operations of *Piper Alpha*. Occidental Petroleum did not replace the OIM who had gone off the job the day before the accident with an experienced OIM, but replaced the individual through temporary promotions with already existing personnel. In addition, the temporary maintenance crews were not completely familiar with the operations and procedures of the offshore installation. These factors are presumed to increase the risk by 50%. Regulating and policing errors by both regulatory bodies (U.K. Department of Energy) and the operator (Occidental Petroleum) led to lax operational procedures aboard the platform. The fact that *Piper Alpha* was allowed to operate under these unsafe conditions without sufficient regulatory control were critical to the disaster particularly with regard to the permit to work system and shutdown of the safety systems during workovers. The effect of regulating and policing on the overall safety of the system is presumed to increase the risk by 100%. The operating policy of Occidental management which allowed the critically high level of production during the major workover to the process system while not sufficiently maintaining the safety system were the most critical factors to the disaster. This high level of risk allowed by Occidental management is related to the increase in risk as a result of operating policy by 200%.

Communications and information were insufficient in that there were no established set procedures to ensure the permit to work system was properly maintained. The critical initiating factor of insufficient information being conveyed between the maintenance crew and the control room crew as to the maintenance status of the process system was a primary contributor to the disaster. The necessity of maintaining proper communication and information during the maintenance on the process system is reflected through an increase in the risk of 100%.

Just before the disaster, most of those aboard the platform were not permanent workers but were maintenance crews just there for the temporary workover. Most were insufficiently prepared for any crisis situation and were unfamiliar with the operations and surroundings.

The impact of this factor on the increased risk to the system is reflected by a 75% increase in the risk to the system.

Other related factors

Other factors related to errors by the front-line operator crew were related to stress, routineness, system, and task complexities as reflected in Table 7.18. Stress was a limited factor in the disaster given the work schedules of performing the platform's workover in a limited time period. There was very little routine in the operation in that the platform had only once been put on Phase 1 operational status while performing a workover. Therefore, the effects of routineness is reflected by a 200% increase in the risk factor. Task and system related factors were similar to those under most workover operations and thus a limited effect upon the system is observed for these related factors. Environmental factors were presumed minimal at the time, but the time of day (approximately) of the operation had a marginal impact on the operation and is reflected in the external environmental factor as increasing the risk by 25%.

Table 7.19 reflects Occidental Petroleum's TLM abilities to sufficiently address each MOE and the MOE related inputs for the maintenance of *Piper Alpha* on the night of the explosions and fires. *Sufficient* (Suff) or *insufficient* (Insuff) inputs for each TLM and MOE combination. The ratings of each MOE for the transit of the vessel are also included.

Table 7.19 - TLM-MOE relations for maintenance of *Piper Alpha* and ratings of MOE factors

	MOE_1	MOE_2	MOE_3	MOE_4	MOE_5	MOE_6	MOE_7	MOE_8	MOE_9
TLM_1	Insuff	Insuff	Insuff	Insuff	Insuff	Insuff	Insuff	Insuff	Insuff
TLM_2	Insuff	Insuff	Suff	Insuff	Insuff	Insuff	Insuff	Insuff	Insuff
TLM_3	Insuff	Insuff	Insuff	Suff	Insuff	Insuff	Insuff	Insuff	Insuff
TLM_4	Suff	Insuff	Insuff	Insuff	Suff	Suff	Insuff	Insuff	Insuff
TLM_5	Suff	Insuff	Suff	Suff	Suff	Insuff	Insuff	Insuff	Suff
MOE rating	Poor	Poor	Poor	Fair	Fair	Poor	Poor	Poor	Fair

Table 7.20 reflects the impact of the system, task, and human factors for the individuals responsible for the maintenance of *Piper Alpha*. A high system complexity was observed as a result of the complex coupling of the system and being in a Phase 1 operation. Task complexities were moderate during the workover in addition to a moderate level of stress for the operation. However, there was little routine in the operation as a result of the system operating in Phase 1 at the time of the disaster. This created problems for control room personnel in identifying, assessing, preventing or mitigating the catastrophic contributors to the loss of fuel containment. External environmental factors were considered moderate as a result of the time of day of operation and internal environmental factors were low.

Table 7.20 - HESIM factors for *Piper Alpha* maintenance

HESIM Factor	
system complexity	high
task complexity	moderate
stress	moderate
routineness	high
environmental (ext)	moderate
environmental (int)	low

Using a factoring constant $k_{ij}=10^3$, the human error risk indices for gas leaks are summarized in Table 7.21. Table 7.22 summarizes the human error safety indices derived for the threat detection and control.

7.3.4.3 Safety index evaluation for *Piper Alpha*

Table 7.23 summarizes the risk index evaluation for the *Piper Alpha* target event of a loss of fuel containment. The impact of human errors conditional upon the disaster is also provided. The primary human error contributors to the loss of fuel containment are observed to be violations and communication-information errors by front-line operators.

Table 7.21 - Conditional risk indices of human errors for maintenance-production model - gas leaks - *Piper Alpha*

Human Errors	Human Error Risk Index (1-Safety Index): Non-process critical		
	No production	Moderate production	High production
human system interface	2.47×10^{-3}	2.96×10^{-3}	2.96×10^{-3}
knowledge-training-expr	2.46×10^{-3}	2.95×10^{-3}	2.95×10^{-3}
0mental physical lapse	2.47×10^{-3}	2.96×10^{-3}	2.96×10^{-3}
violations	2.47×10^{-3}	2.96×10^{-3}	2.96×10^{-3}
job design	2.46×10^{-3}	2.96×10^{-3}	2.96×10^{-3}
communication-information	2.38×10^{-3}	2.86×10^{-3}	2.86×10^{-3}
Human Errors	**Human Error Risk Index (1-Safety Index): Process critical**		
	No production	**Moderate production**	**High production**
human system interface	3.95×10^{-3}	4.87×10^{-3}	9.25×10^{-3}
knowledge-training-expr	3.94×10^{-3}	4.86×10^{-3}	9.23×10^{-3}
mental physical lapse	3.95×10^{-3}	4.88×10^{-3}	9.26×10^{-3}
violations	3.95×10^{-3}	4.87×10^{-3}	9.25×10^{-3}
job design	3.94×10^{-3}	4.86×10^{-3}	9.24×10^{-3}
communication-information	3.81×10^{-3}	4.70×10^{-3}	8.92×10^{-3}

Table 7.22 - Conditional risk indices of human errors for maintenance-production model - detect and control - *Piper Alpha*

Human Errors	Risk Index (1-Safety Index) detection and control
human system interface	1.16×10^{-3}
knowledge-training-expr	1.16×10^{-3}
mental physical lapse	1.16×10^{-3}
violations	1.17×10^{-3}
job design	1.16×10^{-3}
communication-information	1.01×10^{-3}

Table 7.23 - Annual risk indices of groundings and collisions and the associated human errors for each event

Event	RI[loss of containment]
loss of containment	1.61×10^{-3}
Human Error	**RI[human error|loss of containment]**
human system interface	1.11×10^{-3}
knowledge-training-exper	1.26×10^{-3}
mental physical lapse	1.12×10^{-3}
violations	2.27×10^{-3}
job design	1.45×10^{-3}
communication-information	2.41×10^{-3}

7.3.5 Evaluating the Maintenance and Production Model -An Example

Organizational and human factors

The following example is a description of Company B; a subsidiary of a large oil company operating three gas production platforms in the North Sea. Company B, has been wrought by many changes at the middle-level management level over the last 5 years. As a result, turnover rates of both management and operators have been high leading to limited experience and knowledge at the middle management and operator level. There are few proactive measures in place with regard to safety standards though the organization does keep pace with regulatory safety requirements. Maintenance has become a particular sore point within the different elements of the organization. Engineers feel that maintenance has led to a number of minor accidents (injury) and major accidents (fatalities) within the last 10 years as a result of accidents that occur while producing and maintaining simultaneously.

Though Company B is a subsidiary of a larger oil and gas production company, they have been left with only limited resources and has had to rely on contractor and sub-contractor organizations to perform many of their full-scale workover maintenance needs. As a result, the maintenance crews are mostly unfamiliar with the platforms since full scale workovers are normally scheduled for every 2 years. Though relatively reliable, the contract and sub-contract crews also suffer from high turnover rates, limited knowledge and experiences with the large range of platform facilities and technologies being used in the region.

The platforms

The three platforms operated by Company B are 15 to 20 years old and are only producing approximately 45% of their maximum capacity attainable. Though they are on the downside of their production capabilities they are marginally profitable. However, they have been deemed by the parent organization as not profitable enough for major safety upgrades and new technological systems to prevent, locate, and mitigate the effects of gas leaks. The control room has limited facilities by which to shutdown any system that may be leaking gas. As a result, the majority of gas detection and control systems must rely on local shutdown for a leak event. In addition, detection of gas leaks rely, to a large extent, upon operators to detect and control them using their experiences and knowledge of the intricacies of the operating system.

7.3.5.1 Non-HOE related factors

See Table 7.17.

7.3.5.2 HOE related factors

For the models discussed above there are two types of human error factors that are quantified: (1) maintenance errors leading to gas leaks, and (2) leak detection and control errors. The maintenance errors (Figure 7.9) are quantified using the HESIM and the detection and control errors are modeled using probability encoding.

7.3.5.2.1 Maintenance errors

Errors in maintenance are the result of the production level and the type of maintenance being performed. Table 7.24 describes the judgment of system, task, and human factor complexities for Company B at each maintenance level. For process critical maintenance, these factors are considered "moderate" to "high". For non-critical maintenance, the effects on maintenance crews are expected to be minimal.

Table 7.24 - HESIM factors for different production and maintenance schedules

		Maintenance Type	
Production Level	HESIM Factor	Non-process critical	Process critical
NONE	System	low	moderate
NONE	Task	low	moderate
NONE	Human Factor[10]	low	low
MODERATE	System	low	moderate
MODERATE	Task	moderate	moderate
MODERATE	Human Factor[10]	low	moderate
HIGH	System	low	high
HIGH	Task	moderate	moderate
HIGH	Human Factor[10]	low	high

Given the information provided in concerning on Company B's organizational factor, human factors, and the platforms, the company is assumed to be a reactive organization that complies to safety standards to keep up with regulatory safety standards with few proactive safety measures being implemented. For this model there have been 10 records of casualties of the gas production fires recorded for Company B's three platforms since they

[10] Human Factors in this case includes both stress and routineness.

had been constructed. In addition, 300 minor and major workovers have been performed of which 8 casualties found to have occurred during simultaneous production and maintenance operations. Table 7.25 is used to derive the safety indices using the HESIM for human errors conditional upon organizational, human factors, system, and environmental factors described above and are summarized in Table 7.26. This model assumes a weighting constant of $k_{ij}=10^3$ for each human error i and organizational error j. After reduction of the production-maintenance influence diagram (Figure 7.9) the safety indices for the gas leak event is summarized in Table 7.27.

Table 7.25 - Safety index criteria for maintenance errors during simultaneous maintenance-production model for Company B

Total number of recorded transits: 300 records
Number of "simul prod-maint" records: 8 records

TLM factors	TLM weight factors
overall commitment to safety	55%
commit to long term safety goals	5%
cognizance	10%
competence	10%
resources	20%
minimum TLM safety index	.55
MOE factors	**Maximum degree of effect (% increase of effect)**
knowledge-training-experience	2.50 (150%)
maintenance	2.00 (100%)
violations	1.50 (50%)
morale-incentive	1.50 (50%)
job design	1.75 (75%)
regulating-policing	1.75 (75%)
operating policy	1.75 (75%)
communication-information	1.90 (90%)
manning	1.50 (50%)
Other factors	**Maximum degree of effect (% increase of effect)**
stress	1.25 (25%)
routineness	1.25 (25%)
system	2.00 (100%)
task	1.50 (50%)
environmental (external)	1.00 (0%)
environmental (internal)	1.75 (75%)

Table 7.26 - Conditional risk indices of human errors for gas maintenance-production model - Company B

Human Errors	Human Error Risk Index (1-Safety Index): Non-process critical		
	No production	Moderate production	High production
human system interface	2.47×10^{-6}	2.96×10^{-6}	2.96×10^{-6}
knowledge-training-expr	2.46×10^{-6}	2.95×10^{-6}	2.95×10^{-6}
mental physical lapse	2.47×10^{-6}	2.96×10^{-6}	2.96×10^{-6}
violations	2.47×10^{-6}	2.96×10^{-6}	2.96×10^{-6}
job design	2.46×10^{-6}	2.96×10^{-6}	2.96×10^{-6}
communication-information	2.38×10^{-6}	2.86×10^{-6}	2.86×10^{-6}

Human Errors	Human Error Risk Index (1-Safety Index): Process critical		
	No production	Moderate production	High production
human system interface	3.95×10^{-6}	4.87×10^{-6}	9.25×10^{-6}
knowledge-training-expr	3.94×10^{-6}	4.86×10^{-6}	9.23×10^{-6}
mental physical lapse	3.95×10^{-6}	4.88×10^{-6}	9.26×10^{-6}
violations	3.95×10^{-6}	4.87×10^{-6}	9.25×10^{-6}
job design	3.94×10^{-6}	4.86×10^{-6}	9.24×10^{-6}
communication-information	3.81×10^{-6}	4.70×10^{-6}	8.92×10^{-6}

Table 7.27 - Risk indices for gas leaks conditional upon production and maintenance schedule - Company B

production level	type of maint	process leak magnitude	RI[gas lk]
high	process critical	sm leak	4.75×10^{-2}
		mod leak	3.96×10^{-3}
		lg leak	1.32×10^{-3}
"	non-process critical	sm leak	4.64×10^{-3}
		mod leak	3.87×10^{-4}
		lg leak	1.29×10^{-4}
moderate	process critical	sm leak	5.87×10^{-3}
		mod leak	4.89×10^{-4}
		lg leak	1.63×10^{-4}
"	non-process critical	sm leak	5.20×10^{-4}
		mod leak	4.34×10^{-5}
		lg leak	1.45×10^{-5}
none	process critical	sm leak	5.17×10^{-4}
		mod leak	4.31×10^{-4}
		lg leak	1.47×10^{-4}
"	non-process critical	sm leak	8.02×10^{-5}
		mod leak	6.07×10^{-6}
		lg leak	2.20×10^{-6}

7.3.5.2.2 Gas detection and control

Error in gas detection and control are conditional upon the size of the leak and the ability of the operators to shut down the system should it be deemed necessary to do so. The HESIM is used to determine the impacts of operator errors in gas detection and control. Table 7.28 describes the judgment of system, task, and human factor complexities for Company B for detection and control of gas leaks.

Table 7.28 - HESIM factors for different production and maintenance schedules

Gas Leak Magnitude	HESIM Factor	Gas leak detection and control
SMALL	System	low
SMALL	Task	low
SMALL	Human Factor[11]	low
MODERATE	System	low
MODERATE	Task	moderate
MODERATE	Human Factor[11]	moderate
LARGE	System	high
LARGE	Task	high
LARGE	Human Factor[11]	high

Given the information provided in concerning Company B's organizational factors, human factors, and the platforms, the company is assumed to be a reactive organization that complies with safety standards to keep up with regulatory safety standards with few proactive safety measures being implemented. There are 8 gas leak records on file that were found to have occurred during simultaneous production and maintenance operations. Table 7.29 is used to derive the safety indices using the HESIM for human errors conditional upon organizational, human factors, system, and environmental factors described above are summarized in Table 7.30. This model assumes a weighting constant of $k_{ij}=10^3$ for each human error i and organizational error j.

After reduction of the detection and control influence diagram (Figure 7.10) the safety indices for loss of fuel containment is summarized in Table 7.31 given the information provided about Company B above. The risk indices for explosions and fires dependent upon gas leak detection and control. These risk indices are to be compared to the risk indices of explosions and fires as a result of implementing management alternatives as described in the following section.

7.3.5.3 Evaluating HOE management alternatives - Gas leak prevention

Detection and control of process leaks are performed both manually (operator) and automatically (system). The ability to detect and control process leaks are dependent upon the sensitivity of the detection system, experience, knowledge and training of the operating crew, and the technology available in the detection and control system.

---

[11] Human Factors in this case includes both stress and routineness.

Table 7.29 - Safety index criteria for gas leak detection and control during simultaneous maintenance-production model - Company B

Total number of recorded transits: 300 records
Number of "gas leak" records: 10 records

TLM factors	TLM weight factors (detection)
overall commitment to safety	20%
commit to long term safety goals	20%
cognizance	20%
competence	20%
resources	20%
minimum TLM safety index	0.50
MOE factors	**Maximum degree of effect (% increase of effect) detection**
knowledge-training-experience	2.50 (150%)
maintenance	2.50 (150%)
violations	1.50 (50%)
morale-incentive	1.50 (50%)
job design	1.25 (25%)
regulating-policing	1.25 (25%)
operating policy	1.25 (25%)
communication-information	1.90 (90%)
manning	1.25 (25%)
Other factors	**Maximum degree of effect (% increase of effect) detection**
stress	1.25 (25%)
routineness	1.25 (25%)
system	1.75 (75%)
task	1.25 (25%)
environmental (external)	1.00 (0%)
environmental (internal)	1.75 (75%)

Table 7.30 - Conditional risk indices of human errors for gas leak detection and control model - Company B

	Human Error Risk Index (1-Safety Index): Detection and control		
Human Errors	**Small leak**	**Moderate leak**	**Large leak**
human system interface	2.67×10^{-6}	3.29×10^{-6}	9.12×10^{-6}
knowledge-training-expr	2.66×10^{-6}	3.29×10^{-6}	9.10×10^{-6}
mental physical lapse	2.66×10^{-6}	3.29×10^{-6}	9.11×10^{-6}
violations	2.67×10^{-6}	3.30×10^{-6}	9.12×10^{-6}
job design	2.66×10^{-6}	3.29×10^{-6}	9.10×10^{-6}
communication-information	2.66×10^{-6}	3.29×10^{-6}	9.10×10^{-6}

Table 7.31 - Risk indices of explosion or fire conditional upon process leak detection and control

leak control	gas leak detection (human)	explosion or fire	Risk Index
lk control	detected	fire	1.43×10^{-2}
"	"	explosion	1.43×10^{-2}
no lk control	"	fire	2.34×10^{-2}
"	"	explosion	2.34×10^{-2}
lk control[12]	not detected	fire	3.11×10^{-2}
"	"	explosion	3.11×10^{-2}

Errors can also be exacerbated by poorly engineered systems that invite errors. Such systems are difficult to construct, operate, and maintain [Melchers, 1987; Ingles, 1985; Moan, 1983]. New technologies can compound the problems of latent system flaws. Complex design, close coupling (failure of one component leads to failure of other components), and severe performance demands on systems increase the difficulty in controlling the impact of human errors even in well operated systems [Perrow, 1984]. Emergency displays have been found to give improper signals of the state of the systems [United Kingdom Department of Energy, 1988b; Perrow, 1984].

Human performance is a function of the lead time available to respond to warnings in the system. Errors are compounded by the lack of effective early warning systems [Paté-Cornell, 1986]. As observed in Figure 7.11, if the lead time is short, there is little time allowance for corrective action before the situation reaches a critical state. On the other hand, if the system is too sensitive causing frequent false alarms, operators will eventually cease to respond to the warning signals.

As a result of the dangers of gas detection and control problems, Company B (at the parent company's request) implemented an extensive training program for control room operators to both prevent and mitigate the consequences of gas leaks (see Chapter 6). The program was directed at increasing human performance by through operator training and retention. Operators were given simulator training for both crisis and normal operations, well trained control room operators were brought in from the parent company. Better incentive programs were developed to attain greater retention of operator crews better team interaction. In addition, the gas detection and control system was upgraded so control room personnel had full and total control of the process system. This also entailed the ability to shut down the production from a centralized point should any process disturbances occur.

The HESIM was used as a framework to model the HOE management program described above. Table 7.32 shows the effect on front-line operators conditional upon system, task, and human factors through better training (normal operations and crisis management), greater knowledge and experience, and process system control upgrades described above. These changes also reduce the relative impact of system, task, and human factors and are estimated in Table 7.33 (see previous maximum degree of effect factors in Table 7.29).

---

[12] This leak control is related to the system automatically shutting down without human intervention.

The safety indices estimated from the HESIM, given the information provided in Tables 7.32 and 7.33, are summarized in Table 7.34.

Table 7.32 - HESIM factors for different production and maintenance schedules

Gas Leak Magnitude	HESIM Factor	Gas leak detection and control
SMALL	System	low
SMALL	Task	low
SMALL	Human Factor[13]	low
MODERATE	System	low
MODERATE	Task	moderate
MODERATE	Human Factor[13]	low
LARGE	System	moderate
LARGE	Task	moderate
LARGE	Human Factor[13]	moderate

Table 7.33 - Safety index criteria for HOE management alternatives for gas leak detection and control - Company B

Error factors	Maximum degree of effect (% increase of effect) detection and control
stress	1.25 (25%)
routineness	1.25 (25%)
system	1.25 (25%)
task	1.10 (10%)
environmental (external)	1.00 (0%)
environmental (internal)	1.75 (75%)

The impact of detection and control management alternatives to reduce the incidence of explosions and fires are summarized in Table 7.35. Significant reductions in the risk indices for both explosions and fires that were detected and controlled (50.1%). Minor reductions were observed for explosions and fires if leaks are not operator controlled. However, as a result of automatic control and shutdown systems, a substantial reduction is observed in the incidence of explosions or fires for non-human controlled shutdown systems (53.7%).

---

[13] Human Factors in this case includes both stress and routineness.

Table 7.34 - Conditional risk indices of human errors for gas leak detection and control model - Company B

Human Errors	Human Error Risk Index (1-Safety Index): Detection		
	Small leak	Moderate leak	Large leak
human system interface	2.67×10^{-6}	2.79×10^{-6}	3.83×10^{-6}
knowledge-training-expr	2.66×10^{-6}	2.79×10^{-6}	3.82×10^{-6}
mental physical lapse	2.67×10^{-6}	2.79×10^{-6}	3.83×10^{-6}
violations	2.67×10^{-6}	2.80×10^{-6}	3.84×10^{-6}
job design	2.66×10^{-6}	2.79×10^{-6}	3.83×10^{-6}
communication-information	2.66×10^{-6}	2.79×10^{-6}	3.83×10^{-6}

Table 7.35 - Risk indices of explosion or fire conditional upon process leak detection and control with HOE management alternatives - Company B

leak control	gas leak detection (human)	explosion or fire	Risk Index for explosions - fires (% increase in safety)
leak control	detected	fire	7.13×10^{-3} (50.1%)
"	"	explosion	7.13×10^{-3} (50.1%)
no leak control	"	fire	2.03×10^{-2} (13.2%)
"	"	explosion	2.03×10^{-2} (13.2%)
leak control[14]	not detected	fire	1.44×10^{-2} (53.7%)
"	"	explosion	1.44×10^{-2} (53.7%)

7.4 TANKER LOADING-DISCHARGE OPERATIONS

The load and discharge models focus primarily upon the proper interface between vessel and docking facility, proper monitoring of load or discharge, and potential of load or discharge system failure (hoses, pumps, etc.). The failure of the system includes both HOE and mechanical failure of the system.

Before any load or discharge operation, a *Declaration of Inspection* (DOI) is required in which a *Pre-Transfer Conference* (PTC) is performed. In the PTC, the details of the transfer operations are discussed. A typical PTC includes:

(1) *Quantity and type of stocks*

(2) *Cargo transfer sequence*

(3) *Cargo transfer rates*

(4) *Anticipated stoppages*

---

[14] This leak control is related to the system automatically shutting down without human intervention.

(5) *Maximum rail pressure*

(6) *Maximum rail temperature*

(7) *Number and speed of ship's pumps to be used*

(8) *Names of personnel involved*

(9) *Transfer details and critical stages*

(10) *Applicable rules*

(11) *Emergency, discharge containment and reporting, shutdown procedures*

(12) *Shift change procedures*

7.4.1 Structuring Primary Events, Decisions, and Actions

The first stage is to determine the target events for the model. The model template should include remedial events associated with the particular class of accidents. For the load and discharge model, the underlying contributing event is the "initiation of loading or discharge". The direct event is the "loss of fuel containment". Loss of fuel containment includes rupture or leakage of hose or loading arm, failure of vessel-dockside interface, overload of tanks, and failure of valves leading to oil discharge. The compounding event is the discharge of oil into the surrounding water. As shown in Figure 7.12, the model the contributing or underlying event is "initiate load or discharge". The direct event is the "loss of fuel containment" and final target event is the "product spill in water".

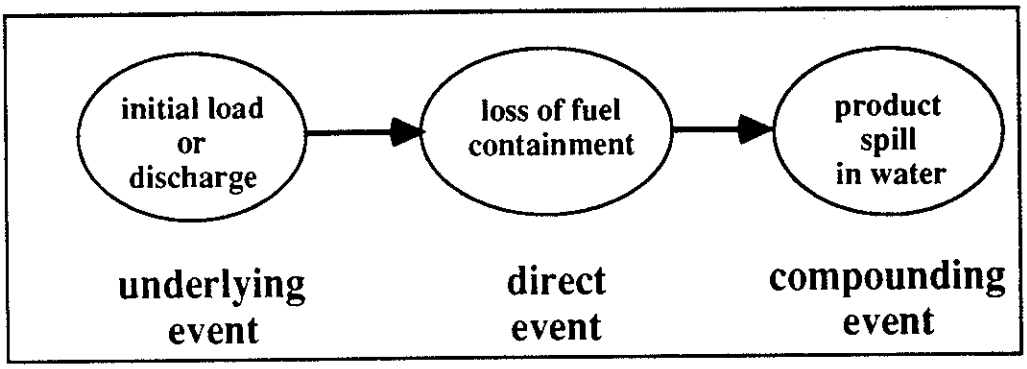


Figure 7.12 - Load and discharge primary accident events

The primary associated decisions and actions that can influence an accident events are the monitoring of the load or discharge by both the vessel crew and the dockside personnel. Crew changes during loading or discharge operations affect the monitoring aspect of the operation. The rate of the load and discharge is a factor which can directly influence the failure of the system. It is assumed that higher rates of loading or discharge increase the probability of a system failure. System failures include hoses, valves, pumps, power plant, and emergency shutdowns. The influences of these factors are shown in Figure 7.13.

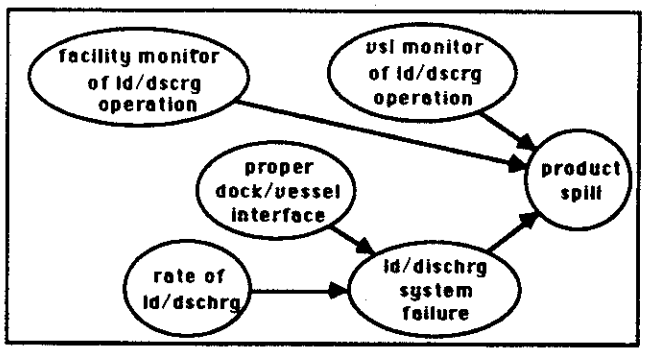


Figure 7.13 - Influence of factors leading to a product spill during load or discharge operation

7.4.2 Relating Relevant Hoe and Environmental Factors

Figure 7.14 is used as a guide in determining the relevant HOE and environmental factors influencing accident events, decisions, and actions. The primary events shown in Figure 7.12 each have contributing HOE and environmental factors. For the underlying-contributing event "initiation of load or discharge", there may be miscommunications (incomplete or inaccurate communications) of any one of the details of the Pre-Transfer Conference. System errors may present wrong information to the operator. Human errors are include miscommunication, lack of training, experience and knowledge of the system, and mental-physical lapses (fatigue, alcohol, drugs, etc.). Morale and incentives of vessel or dockside operators may affect the transfer operation. Experiences of marine facility investigators have shown that loading and discharge problems are generally the result of miscommunication between parties involved (tanker crews, barge crews, and shore personnel), lack of training, experience, and knowledge of the system [California State Lands Commission, 1992].

Organizational factors influencing the underlying-contributing events are operating policies which affect the decisions made by front-line operators. Operator views toward safety, operating policy, and internal regulating and policing vary between crews and organizations. Operators with limited resources and low commitments to safety may be more willing to violate operating policies or regulations. Regulatory errors such as insufficient regulating or policing can contribute to an accident scenario.

The direct accident event, "loss of fuel containment" may be the result of system errors (failure of operating console or inability to sufficiently read the console). Operators may lack the knowledge, training, or experience. In addition, insufficient manning, or other duties may distract them (job design) from the load or discharge operation. Similar to the underlying and contributing causes, miscommunications between personnel leads to the loss of fuel containment by loading or discharging at an improper rate, time, or duration. Lack of a commitment to maintenance from the operators potentially contribute to the failure of the system.

The compounding accident event "product spill in water" can be the result of a lack of awareness leading to a loss of fuel containment while monitoring. This may be due to system errors (no early warning), inattention or fatigue (mental-physical lapse), lack of contingency plans by the operator (emergency shutdown system or procedure), or a lack of proper maintenance.

Environmental factors (i.e. wind, waves, etc.) are observed to affect the offshore spread mooring operations by influencing the mooring-vessel interface of the operation. Vessels passing in close proximity to another vessel during load or discharge operations at a docking facility can create substantial vessel motions. Both of these factors can produce stresses on hoses or riggings as a result of dynamic motions of the vessel. Snow, ice, or cold can directly affect the operators abilities to properly prepare the dock-vessel interface (e.g. snow and ice on tanker load and discharge manifolds, dockside loading arms, or hoses).

Figure 7.15 shows the influence diagram for loading and discharge operations. The human and system errors directly influence the terminal and vessel monitoring of the load or discharge operation. Environmental conditions are observed to affect the mooring-vessel interface described above. Table 7.1 shows the outcomes for each factor described in the model.

(1) *Environmental conditions*. Environmental operating conditions are described as a state variable (probability) since the load and discharge operations occur under varying conditions. Waves at an offshore spread mooring may make it difficult to have a proper hose-vessel interface. Extreme cold conditions can affect the vessel interface.

(2) *Human errors*. Human errors are affected by the environmental operating conditions. Extreme cold may affect the crew's actions in interfacing the vessel with the load or discharge facility.

(3) *System errors*. System errors may occur as a result of extreme environmental conditions. Gauges may freeze or become difficult to read in extreme weather.

(4) *Load-discharge facility monitoring*. This is the monitoring of vessel operations by the dockside, spread mooring, or marine facility crew. The monitoring may be directly affected by wrong information resulting from system errors. Human errors may be the result of a lack of experience, training, or knowledge of the monitoring system. Inattention, fatigue, morale, or incentives may prevent sufficient monitoring of load or discharge operations.

(5) *Load-discharge vessel monitoring*. The monitoring of the vessel operation by the tanker crew. The conditions are the same as those of the facility crews.

(6) *Proper dock vessel interface*. The dock-vessel interface is the linking of the shoreside (or mooring) hoses or loading arms with the vessel. The failure of the interface leads to a spill event.

(7) *Load-discharge rate*. The higher the load or discharge rate, the larger the spill size. The discharge rate also influences the load and discharge system failure. It is assumed that the higher the load or discharge rate, the greater the chances of a system failure (hose bursting, leak at the flange assembly, etc.).

(8) *Load-discharge system failure*. Entails having the system fail such that a loss of fuel containment is observed. System failures are the result of facility-vessel interface and the load or discharge.

(9) *Product spill*. The product spill is affected by a system failure and by the proper monitoring of the system. If monitoring of the system is not sufficient, there is no spill intervention. If monitoring is sufficient, it is assumed the system is shut down and no spill occurs.

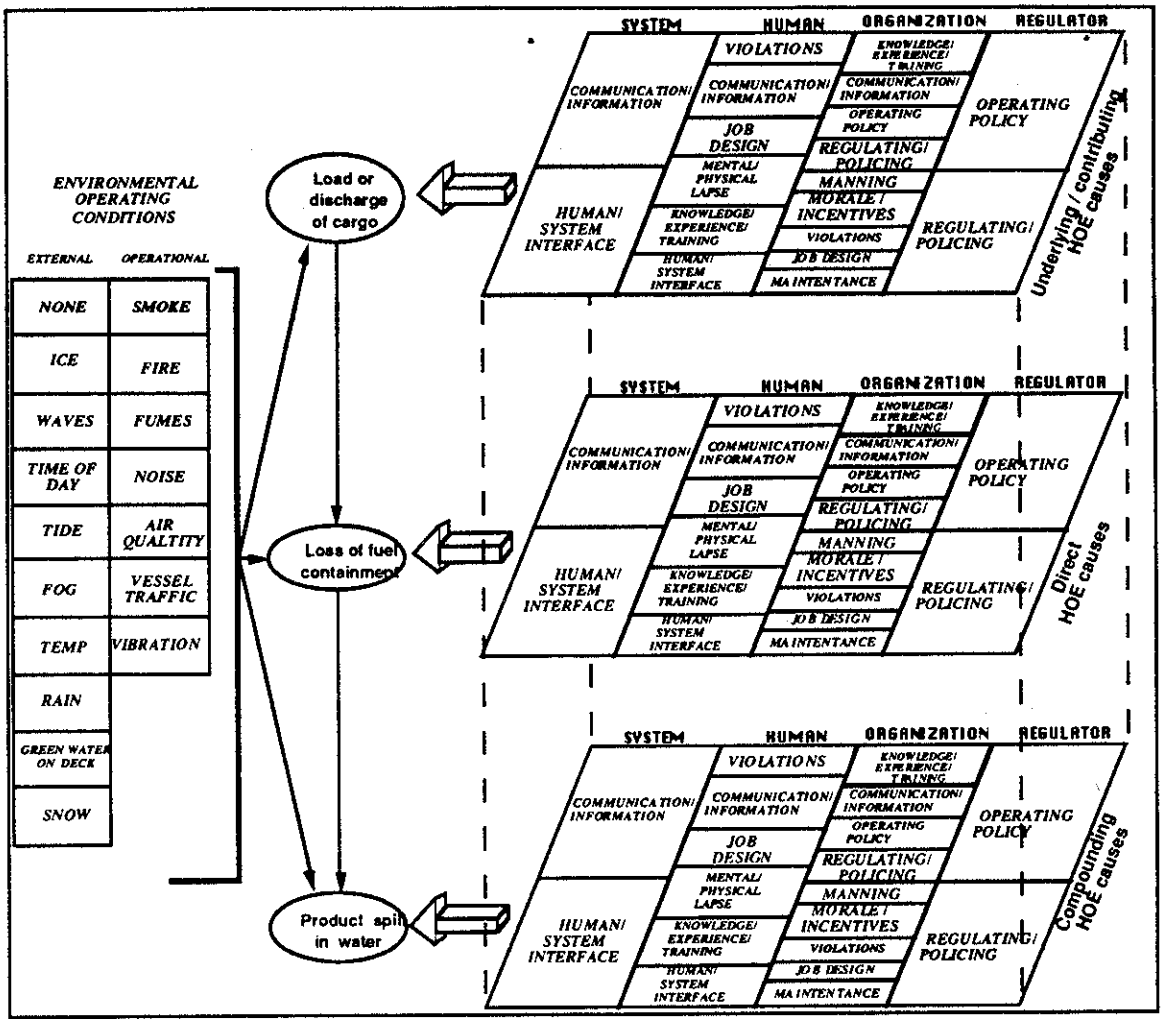


Figure 7.14 - Influence of HOE and environmental factors upon primary events for tanker load or discharge

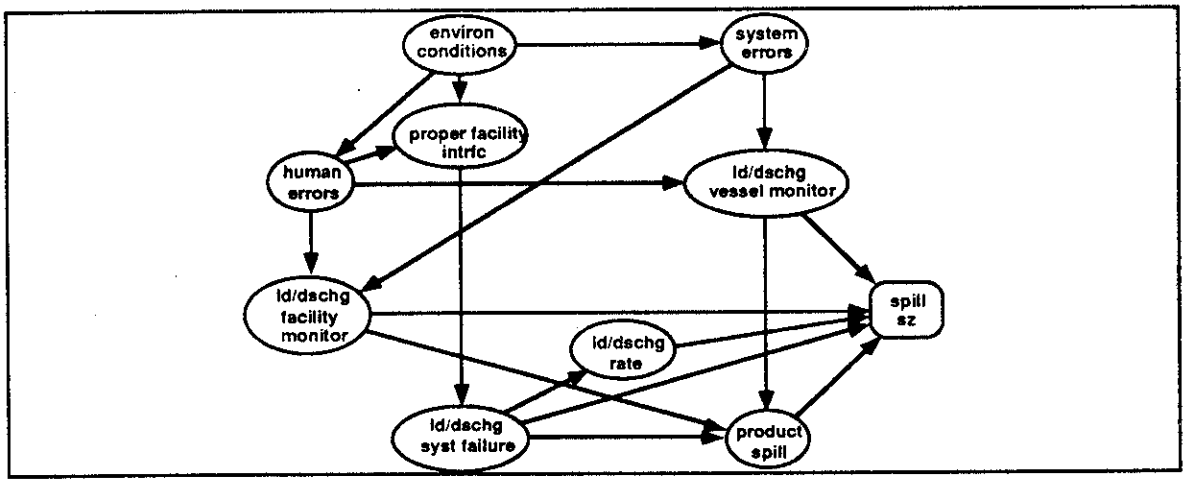


Figure 7.15 - Tanker load and discharge influence diagram

Table 7.36 - Outcomes for load and discharge influence diagram

human errors	system errors	spill sz
none	*none*	*0.0*
hum-syst intrfc	*comm-info*	*10.0*
knwl-trn-expr	*hmn syst intrface*	*50.0*
mntl-phys lps		*100.0*
violation	**proper facility interface**	*250.0*
job dsgn	*proper interface*	*500.0*
comm-info	*improper interface*	*1000.0*
load-dschrg rate	**product spill**	**ld-dschrg facility monitor**
none	*spill*	*monitor*
moderate	*no spill*	*no monitor*
high		
ld-dschrg system failure	**ld-dscrg vessel monitor**	**envrion conditions**
operational	*monitor*	*none*
failure	*no monitor*	*waves*
		wind
		ice

(10) *Spill size.* Spill size (barrels or bbls) is the result of whether the load and discharge were being monitored, and a system failure occurred. Spill size is modeled as a value node with a distributions of outcomes dependent upon the level of monitoring and load or discharge rates, should a failure occur.

7.4.3 Evaluating the Load-Discharge Model - An Example

Company C is the owner and operator of a 5 point offshore spread mooring facility in Southern California. The company services both their own vessels and other vessels that are in need of discharge services. The majority of vessels that use these facility are Trans-Alaska Pipeline Service (TAPS) trade tankers transiting between Southern California and Alaska. Company C has been operating for 15 years and have had no product spills that have gone into the water. Company C, though relatively proactive, has collected no detailed records of spills. However, as a result of regulatory requirements, Company C must perform case study Though Company C feels comfortable with the reliability of their company personnel, they have a growing concern regarding foreign flagged vessels operating in their mooring facility. Since these case studies are required, Company C would like to use the opportunity to assess alternatives that can assist them in reducing the risks of spill at the spread mooring site when loading or discharging foreign flag vessels.

Though Company C has not collected much HOE data of operational problems at the marine facility, there is a plethora of technical and managerial expertise that would allow them to make reasonable judgments as to the risks of load or discharge spills at the mooring sight.

Organizational and human factors

Company C has been in business in the Southern California area for well over 60 years and has had a reputation of being a proactive company that keeps abreast of any operational problems within their organization. Company C is particularly proud of the fact that they have designated crews to operate their marine facilities. Fair pay, benefits, and close interaction between management and operators has led to high morale within the organization.

Operators are well trained, knowledgeable, and experienced. Facility crews have been trained and experienced in different parts Company C's business. Most operator crews rotate into the marine facility job from the company's refinery operations. In addition, the crew members are normally rotated through the marine facilities operations as teams and not individually to maintain a higher level of teamwork.

The mooring masters who are responsible for securing the vessel, its mooring lines, and the load-discharge interfacing. Each of Company C's 4 mooring masters have had a minimum of 5 years experience as mooring master and has a master's license.

The operations

Company C operates with strict safety guidelines for both their own ships and for ship operations by any other company that wishes to use their facilities. Operators and load and discharge crews adhere strictly to the safety requirements. Though Company C is assured of the safe operating conditions of their ships, they have had occasional language and communication problems with other company's foreign flagged vessels that use their facilities.

Though they are required to have English speaking personnel aboard vessels using Company C's facilities, many foreign flagged vessels have only one or two English speaking officers. For offshore spread moorings the vessel crew is assumed to have a greater responsibility in visible monitoring of the interface between the loading and discharge lines. Though the proper information is communicated at the time of initiation of operations, many times the English speaking officers may be detained with other duties and are not available when the tanks are being stripped or topped off. These problems have been of particular concern during bunkering operations. Though no oil has been spilled in the ocean, two close calls within the last year have made Company C uneasy as to the safety of operations.

Recently, mooring masters have had particular problems communicating how to connect both mooring lines and hoses. Many times mooring masters find themselves overwhelmed with duties related to securing of mooring lines and vessel maneuvering when working with foreign crews and during averse weather conditions. Mooring masters have complained in certain instances that it would be advantageous to have additional assistance in mooring duties when working with foreign crews and/or during averse weather conditions.

Company C has recently invested in upgrading the load-discharge monitoring, safety shutdown systems, and load and discharge hoses for the terminal. These systems can be easily monitored and shutdown by terminal personnel during load or discharge operation.

7.4.3.1 Non-HOE (system) related factors

Given the influence diagram template and the load and discharge system discussed above and shown in Figure 7.15, the probability distributions are summarized for the reliability of the system in Table 7.37. The probability distributions were derived using heuristic judgments and system reliability information (loading system failures, hoses, loading arms, etc.) was used to arrive at the probability distributions presented in Table 7.37. Any factor in Table 7.37 can be modified and adjusted to account for the specifics of any unique operation.

Table 7.38 summarizes the magnitude of spill sizes conditional upon monitoring, load discharge system failures, discharge rates and incidence of spill. This model assumes the largest spill would be 1,000 bbls and catastrophic spills are not accounted for.

7.4.3.2 HOE related factors

To assess the probabilities of human errors and related factors, the following assessments are made as a result of experience and judgments of experts familiar with load and discharge operations integrated with the operational profile of Company C. In accordance with the influence diagram model in Figure 7.15, human errors are the direct result of environmental and system factors and indirectly associated with organizational errors and other operational factors that describe Company C in Section 7.4.3.

Table 7.39 summarizes the probability distributions for: (1) human errors conditional upon environmental and system factors, (2) load-discharge monitoring conditional upon human errors, and (3) proper vessel-system interfaces conditional upon human errors. Provided the information describing the spread mooring operation and description of Company C, the primary human factors that are of concern are human-system interface and communication-information errors. The probability distributions in Table 7.39 reflect the judgments of these types of human errors.

7.4.3.3 Evaluation of the model

Table 7.40 summarizes the results reducing the loading-discharge influence diagram shown in Figure 7.15. It has been established that the probability of a spill reaching the water is 1.39×10^{-3} (or 1.39 times per 1000 operations). The expected value of the spill is small at 1.82 barrels with standard deviation of 3.97 barrels. Using a cost standard of $4,500 per barrel of oil spilled, the expected cost would be $8,190.00 with a standard deviation of the cost being $17,865.00.

7.4.4 Evaluating HOE Management Alternatives - Additional Mooring Master

As mentioned above, Company C has been looking for alternatives that would increase the safety of the spread mooring operation when foreign flagged vessels are using their facilities. An alternative under consideration would be to assign a deck master to assist the mooring master in his or her duties. The duties of the mooring master entails advising the vessel master on approaching and departing the berth, and mooring the vessel. All maneuvering within the mooring area is done only in accordance with the advice of the mooring master. The addition of a deck master to monitor and advise all placing of mooring lines and anchors, load and discharge interfacing between vessel and connecting hoses would increase the reliability of the load-discharge operation. All decisions and actions of the deck master are in accordance with the advice of the mooring master. The addition of the deck master is assumed to increase the reliability of loading and discharge operation in the areas of: (1) knowledge, training, and experience, (2) vessel-mooring interface, (3) vessel monitoring of operation, and (4) product spill.

The alternative of assigning a mooring master is reflected in Table 7.41. When assigning the deck master to assist the mooring master in his or her duties for foreign flagged vessels, it will have a direct effect upon five types of human errors: (1) knowledge, training, and experience, (2) mental physical lapses, (3) violations, (4) job design, and (5) communication and information. The incidence of mental and physical lapses are reduced as a result of the deck master being on the deck at all times monitoring the mooring lines, the load-discharge interface, and the vessel's deck crew. Violations, whether intentional or unintentional, are less likely when a deck master is on site monitoring operations. Since the deck master's responsibilities exclusively entail the deck operations, the incidence of job design errors are reduced. It is also the responsibility of the deck master to communicate all loading and discharge information between the mooring master, vessel

master, and the terminal facility resulting in a reduction in the incidence of communication and information errors.

As observed in Table 7.42, by using a deck master on foreign flagged vessels, Company C is able to reduce the incidence of oil spills by 26.6%. The overall incidence of human errors was reduced by 36.1%. Substantial reductions in the incidence of knowledge, training, experience, mental-physical lapses, job design, and communication-information errors are observed. The expected value of the spill was reduced by 30.1% ($5,670.00 at $4,500 per barrel spilled).

7.5 OFFSHORE CRANE OPERATIONS

Crane accidents have continued to plague the offshore industry for many years. Between 1971 and 1983, 50 crane accidents were reported of which 35 were the effect of human error resulting in 37 fatalities and 26 injuries [U.S. Department of Interior, 1984]. The intent is to develop an offshore crane model that focuses primarily upon crane operator and rigging crew errors to determine how HOE management alternatives can reduce the incidence of crane related casualties.

7.5.1 Structuring Primary Events, Decisions, and Actions

The primary crane operations are transporting equipment and materials between offshore supply vessels and a platform for transporting equipment and materials across a platform deck for normal production and maintenance operations (e.g. well pipe, compressors, etc.). The first stage is to determine target events in order to structure related events, decisions, actions, HOEs, system errors, and environmental factors that influence the important factors. The model template include the remedial events which are specific to the casualty class of crane accidents.

As shown in Figure 7.16, the primary underlying event is the "initiation of crane operations"., the direct event is the "loss of load control", and the compounding event is the "loss of load". Before any crane transfers cargo, machinery, or equipment, a pre-transfer conference to establish the load type, loading procedure, environmental conditions, and establish if any other activities is held within the vicinity of the loading or discharge operation. The loss of load control is defined as the inability to safely control the movement of the load by the operator or rigger. The loss of load is defined as an inadvertent, uncontrolled, or accidental dropping of crane loads. Rigging and operational failures include both human and system (mechanical) errors.

The EDAs that can influence accident events are rigging or operational failures. Riggings may be improperly arranged (rig or offshore supply vessel crew) or the riggings may be improperly maintained (rig crew). Operating failures are defined as mechanical crane failures during operation or failures resulting from crane operator errors. One critical factor for crane operations is whether the crane operator is in the line of sight (LOS) of the job being performed. A lack of visual cues for the operator can heighten the risk of losing load control. Each of these operational factors resulting in losing load control are shown in an influence diagram representation in Figure 7.17.

Table 7.37 -Load-discharge influence diagram model probability distributions excluding human error factors

Environmental factors

	P[environmental]
None	0.97
Wind	0.005
Waves	0.020
Temperature	0.005

Environmental factors influencing system reliability

	P[system error | environmental]	
	communication-information	human system interface
None	0.002	0.002
Wind	0.003	0.004
Waves	0.005	0.003
Temperature	0.04	0.07

Load-dschg rate

	P[rate]
None	0.20
Moderate	0.40
High	0.40

Load-dschg system failure

	P[system failure | rate,interface]		
Dock vessel-interface	low	moderate	high
Proper	0.001	0.001	0.005
Improper	0.10	0.25	0.40

Product spill conditional upon load and discharge system failure

ld-dschg vessel monitor	ld-dschg facility monitor	P[spill | monitoring, system operational]
Proper	Proper	0.05
Improper	"	0.50
Proper	Improper	0.50
Improper	"	1.00

Table 7.38 - Spill magnitudes for load and discharge model

vessel monitoring	facility monitoring	discharge rate	ld-dschg system failure	spill	spill size (bbls)
monitor	monitor	low	operates	spill	10.00
"	"	moderate	"	"	25.00
"	"	high	"	"	50.00
"	no monitor	low	"	"	25.00
"	"	moderate	"	"	50.00
"	"	high	"	"	100.00
no monitor	monitor	low	fail	"	50.00
"	"	moderate	"	"	100.00
"	"	high	"	"	250.00
"	no monitor	low	"	"	250.00
"	"	moderate	"	"	500.00
"	"	high	"	"	1000.00
monitor	monitor	low	"	"	25.00
"	"	moderate	"	"	50.00
"	"	high	"	"	100.00
"	no monitor	low	"	"	50.00
"	"	moderate	"	"	100.00
"	"	high	"	"	250.00
no monitor	monitor	low	operates	"	25.00
"	"	moderate	"	"	50.00
"	"	high	"	"	100.00
"	no monitor	low	"	"	50.00
"	"	moderate	"	"	100.00
"	"	high	"	"	250.00

Table 7.39 - Human error related probabilities for load-discharge model

Human errors conditional upon environmental conditions and no system errors

	P[human error| environ, no syst errors]			
Human Error	**none**	**waves**	**wind**	**cold**
none	0.900	0.800	0.800	0.800
human system interface	0.015	0.025	0.025	0.025
knowledge-training-experience	0.015	0.050	0.050	0.050
mental physical lapse	0.010	0.015	0.015	0.065
violations	0.010	0.010	0.010	0.010
job design	0.025	0.025	0.025	0.025
communication-information	0.025	0.075	0.075	0.025

Human errors conditional upon environmental conditions and comm-info system errors

	P[human error| environ, comm-info syst errors]			
Human Error	**none**	**waves**	**wind**	**cold**
none	0.800	0.700	0.700	0.700
human system interface	0.025	0.075	0.075	0.075
knowledge-training-experience	0.050	0.050	0.050	0.050
mental physical lapse	0.015	0.015	0.015	0.015
violations	0.010	0.010	0.010	0.010
job design	0.025	0.025	0.025	0.025
communication-information	0.075	0.125	0.125	0.125

Human errors conditional on environmental conditions and hum-syst intrfc system errors

	P[human error| environ, hum-syst intrfc errors]			
Human Error	**none**	**waves**	**wind**	**cold**
none	0.800	0.700	0.700	0.700
human system interface	0.025	0.075	0.075	0.075
knowledge-training-experience	0.050	0.050	0.050	0.050
mental physical lapse	0.015	0.015	0.015	0.015
violations	0.010	0.010	0.010	0.010
job design	0.025	0.025	0.025	0.025
communication-information	0.075	0.125	0.125	0.125

Table 7.39 - Human error related probabilities for load-discharge model (cont.)

Load-discharge facility monitoring conditional upon human errors

	P[sufficient monitoring| human error]		
Human Error	**none**	**comm-info**	**hum syst intrfc**
none	1.000	0.950	0.950
human system interface	0.900	0.800	0.800
knowledge-training-experience	0.930	0.850	0.850
mental physical lapse	0.980	0.950	0.950
violations	0.930	0.900	0.900
job design	0.900	0.850	0.850
communication-information	0.995	0.750	0.750

Vessel monitoring conditional upon human errors

	P[sufficient monitoring| human error]		
Human Error	**none**	**comm-info**	**hum syst intrfc**
none	1.000	0.950	0.950
human system interface	0.850	0.750	0.750
knowledge-training-experience	0.750	0.650	0.650
mental physical lapse	0.800	0.725	0.725
violations	0.800	0.725	0.725
job design	0.750	0.650	0.650
communication-information	0.900	0.850	0.850

Vessel-system interface conditional upon human errors

	P[proper vessel interface| human error]			
Human Error	**none**	**waves**	**wind**	**cold**
none	0.950	0.900	0.900	0.900
human system interface	0.900	0.750	0.750	0.650
knowledge-training-experience	0.850	0.800	0.800	0.750
mental physical lapse	0.900	0.800	0.800	0.700
violations	0.950	0.900	0.900	0.900
job design	0.850	0.750	0.750	0.750
communication-information	0.900	0.800	0.800	0.800

Table 7.40 - Tanker load-discharge spread mooring model results

Operation	P[spill]-operation	EV[spill] (bbl)	SD[spill]
Spread mooring	1.39×10^{-3}	1.82	3.97

Human Error	P[human error|spill]
none	0.546
human system interface	0.060
knowledge-training-experience	0.105
mental-physical lapse	0.037
violation	0.021
job design	0.170
comm-info	0.062

Table 7.41 - Human error probabilities for load-discharge model when requiring services of a deck master

Vessel monitoring conditional upon human errors

	P[sufficient monitoring|human error]		
Human Error	none	comm-info	hum syst intrfc
none	1.000	0.950	0.950
human system interface	0.850	0.750	0.750
knowledge-training-experience	0.950	0.850	0.850
mental physical lapse	0.900	0.850	0.850
violations	0.850	0.800	0.800
job design	0.750	0.650	0.650
communication-information	0.990	0.950	0.950

Vessel-system interface conditional upon human errors

	P[proper vessel interface| human error]			
Human Error	none	waves	wind	cold
none	0.950	0.900	0.900	0.900
human system interface	0.900	0.750	0.750	0.650
knowledge-training-experience	0.950	0.900	0.900	0.850
mental physical lapse	0.990	0.900	0.900	0.900
violations	0.950	0.900	0.900	0.900
job design	0.950	0.900	0.900	0.900
communication-information	0.950	0.900	0.900	0.900

Table 7.42 - Tanker load-discharge spread mooring model results when assigning deck master

Operation	P[spill] (% change for w-deck master)	EV[spill] (bbl) (% change for w-deck master)	SD[spill]
Spread mooring	1.02×10^{-3} (26.6%)	1.26 (30.1%)	2.49

Human Error	P[human error|spill] (% change for w-deck master)
none	0.743 (36.1%)
human system interface	0.081 (35.0%)
knowledge-training-experience	0.030 (-71.4%)
mental-physical lapse	0.007 (-81.1%)
violation	0.025 (16.0%)
job design	0.087 (-48.8%)
comm-info	0.027 (-56.5%)

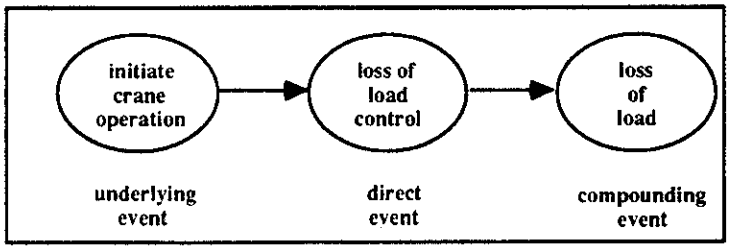


Figure 7.16 - Crane operation primary accident events

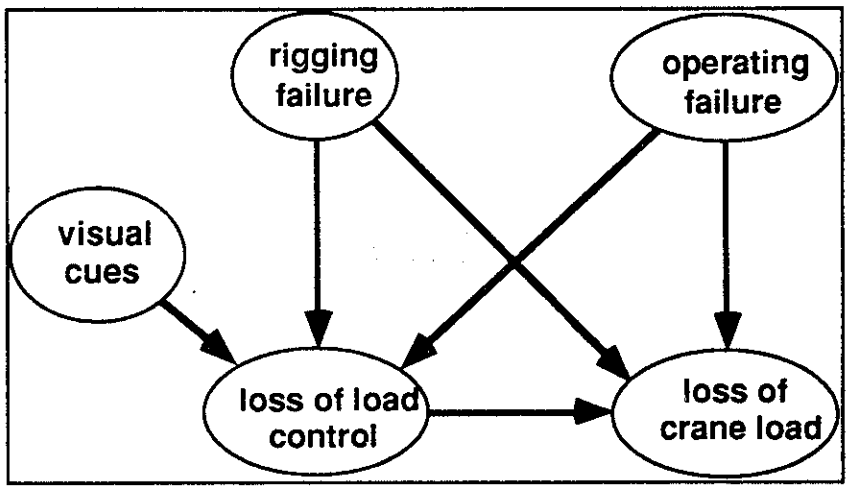


Figure 7.17 - Offshore crane accident influence diagram

7.5.2 Relating Relevant HOE and Environmental Factors

Figure 7.18 is used as a guide in determining the relevant HOE and environmental factors influencing accident initiating EDAs. The events shown in Figure 7.16 each have related HOE and environmental factors that contribute to casualty causing scenarios. For the

underlying event "initiation of crane operation", human errors such as operator violations (unsafe procedure, willful overload of crane, etc.), miscommunication between crane operators and platform personnel, lack of training, experience, or knowledge of the system, or cognizance of other activities being performed within proximity of the crane operation. Operating policies of the organization, lack of incentives, and limited regulating and policing of crane operations contribute to violations and unsafe operations.

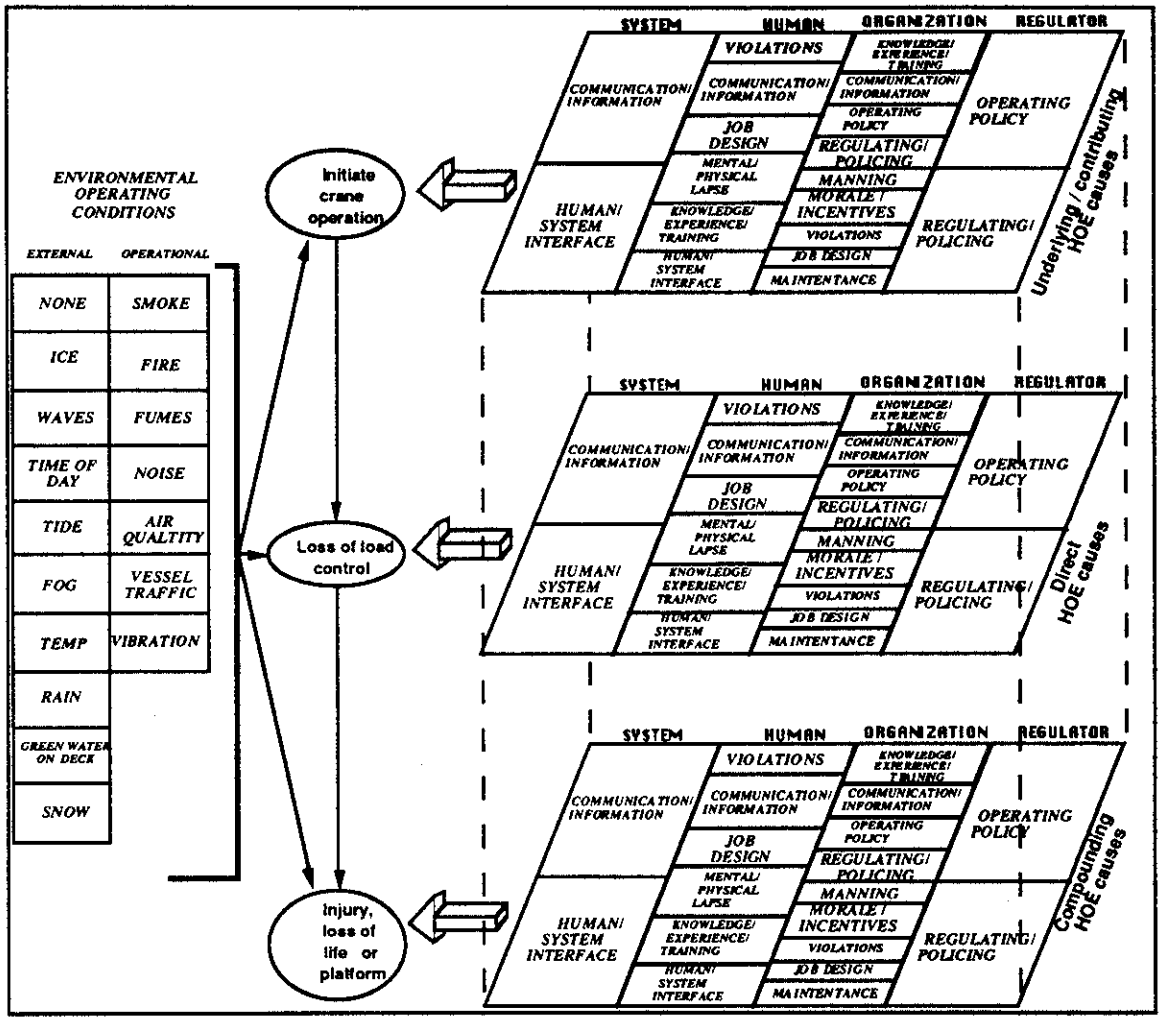


Figure 7.18 - Influence of HOE and environmental factors upon primary events of an offshore crane operation

The direct accident event, "loss of load control" may be the result of system errors (failure of crane display panel or inability to sufficiently read the display panel). Human errors can be the result of a lack the knowledge, training, experience, insufficient manning, or other duties may distract them (job design) from the operation. A lack of a commitment to maintenance from the organization or operating crews may contribute to the failure of the system. Environmental factors such as wind and waves can illicit vessel motions while loading or off-loading and contribute to rigging and operating problems. Vessels heaving

poses a particular problem for cranes loading or off-loading offshore supply vessels (OSVs) resulting in impact loads on riggings that increase the risk of failure.

The compounding accident event "loss of load" can be the result of loss of load control or operator errors. Trained and experienced operators are assumed to function better in crises involving the loss of load control. The crane control system or riggings may be inadequate to allow the operator to bring the load under control. Environmental factors affect the "loss of load" event in the same manner as the "loss of control".

The human and system errors directly influence the operating and rigging failures. The operator not being within the LOS of the lift operations lack of visual cues to maintain load control. Operator and rigging failures directly influence the loss of load control and crane load. The following summarizes the outcomes for each factor described in the influence diagram template in Figure 7.19 and are shown in Table 7.43.

(1) *Environmental conditions.* The environmental operating conditions are described as a state variable since the conditions will vary between locations and random sea states (for waves).

(2) *Human errors.* Human errors are affected by the environmental operating conditions and the crane operation being performed. Crane operations in difficult sea states are presumed to be a non-routine and stressful operation. Most other operations are presumed to be normal low stress routines unless outside of the LOS of the operator.

(3) *Crane operation type.* The crane operation type is categorized into deck-deck operations and vessel-deck operations. Crane booms will swing over the platform and the vessel dependent upon the operation.

(4) *Rigging failure.* The rigging failure is the failure of the rigging system such that it affects the loss of load control or loss of crane load. A rigging failure is the result of the type of crane operation, human errors, and environmental conditions.

(5) *Operating failure.* Operating failure is related to a human initiated failure which results in a loss of load control or loss of load. The operating failure is influenced by the type of crane operation, human errors, and the environmental conditions.

(6) *Loss of load control.* The loss of load control is defined as the inability to safely control the movement of the load by the operator or rigger.

(7) *Loss of load.* The loss of load is defined as the inadvertent, uncontrolled, or accidental dropping of crane loads.

(8) *Loss location.* The loss location is the location where the crane load is dropped. The loss location is dependent upon the span of the crane boom and where crane operations are normally performed.

(9) *Loss size.* Loss size is a value node representing cost values as a function of the load loss (load control or load drop).

7.5.3 Evaluations of Crane Operation Model - An Example

Company D is an international oil company that operates 8 offshore production platforms off of the coast of California. Company D has a regional office in the Los Angeles basin area that is responsible for the maintenance, operation, and transport of oil to shore. Company D has recently become concerned with a number of near misses and minor

accidents that have been related to the age and maintenance of the cranes. Though Company D is confident with respect to the commitment to safety of its own personnel, there have been small casualties and near misses as a result of offshore supply vessel crews having limited training and experiences in rigging loads for the vessel-deck operation.

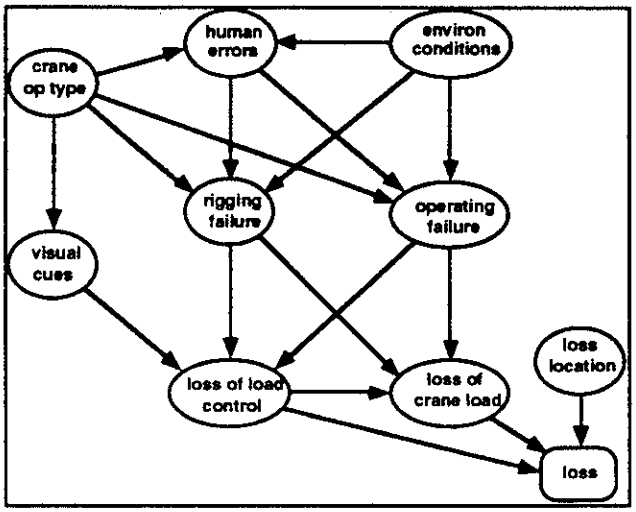


Figure 7.19 - Offshore crane accident influence diagram with HOE factors

Table 7.43 - Outcomes within each node of crane accident influence diagram

lack of visual cues	**system errors**	**environmental conditions**
within line of sight (LOS)	*none*	*none*
no line of sight (no LOS)	*comm-info*	*waves*
	hmn syst intrface	*wind*
loss of load control		
load control	**human errors**	**rigging failure**
no load control	*none*	*none*
	hum-syst intrfc	*operational*
loss of crane load	*knwl-expr-trng*	*failure*
loss of load	*mntl-phys lapse*	
no loss of load	*job design*	**operating failure**
	violations	*none*
loss of crane load	*comm-info*	*moderate*
deck-deck		*high*
vsl-deck		

After some investigation, Company D has realized that the layouts on 5 of the platforms have made it particularly difficult to be in a continual line of sight between the operator crane booth and the load being handled. It is particularly difficult for crane operators to see when loading or discharging offshore supply vessels as a result of the crane's position. Company D has found it necessary to rely heavily upon other platform personnel to assist crane operators in handling cargo. To the surprise of Company D's management, they have realized that most crane operators involved in the incidents are experienced and well trained. Company D has also found that most of the casualties have been the result of

miscommunications between crane operators and the platform personnel responsible for assisting them in their operation.

The cranes

For the eight platforms, there are a total of 14 cranes that range between 5 and 15 years of age and were purchased from two different companies. A particular concern of the OIMs has been that the skills needed to operate the two types of cranes vary significantly. Crane X is an older style model which is less automated and depends on the operator to be significantly more skilled than operating Crane Y. Crane Y is fully automated and its controls are fail-safe in that if the operator was to remove his or her hands and feet from the controls, all operations would cease. Such fail-safe features are not included for Crane X.

Though an effective maintenance program has been implemented by Company D, the down time for the cranes has increased drastically over the last 2 years. The percentage of time that cranes are out of service has risen to 25%. This has put increasing pressure on Company D to keep the cranes operational.

Managing the problem

These near misses and minor casualties have moved Company D to inquire into alternatives that can assist them in reducing the risks of crane related accidents. Company D realizes it must perform a human reliability based analysis to determine the risks of crane operations on a case by case basis. Company D has determined that it would like to address the problem of visual cues for crane operators to determine how the operator may reduce the risks of accidents if the operator is able to always be in visual contact of the operation being performed.

7.5.3.1 Non-HOE related factors

The study is initiated with *Platform G*, a platform that Company D has had the greatest frequency of crane related problems. Given the layout of the platform, environmental factors, and operational procedures, and reliability based data on operational and rigging failures, Company D has estimated measurements for casualty related factors for the crane operation influence diagram (Figure 7.9) and are summarized Table 7.44.

7.5.3.2 HOE related factors

Given the profile of Company D, the primary contributing human errors that can lead to accident scenarios can be identified as: (1) human system interface, and (2) communication-information errors. As a result, judgments of human error frequencies by crane operators, OIMs, engineers, and other personnel on *Platform G* have led to the human error probabilities summarized in Table 7.45.

As observed in Table 7.45, errors resulting from human system interface problems and communication-information are more prevalent to accident scenarios. The incidence of errors are observed to be higher for vessel-deck crane operations; particularly those outside of line of sight of the crane operator. Rigging and operational failures conditional upon human errors for vessel-deck operations reflect the deficiencies of offshore supply vessel crews to properly rig loads.

7.5.3.3 Evaluating the model

Table 7.46 summarizes the results from the crane operations influence diagram. The loss of load control is observed in 8.2% of crane operations (8.2 of 100 operations) and a loss of load in 4.4% of crane operations (4.4 of 100 operations). Human system interface, knowledge, training, and experience, and communication-information problems are the primary human error causes to the loss of load control and loss of load target events.

Table 7.44 -Crane operation influence diagram model probability distributions excluding human error factors - Company D

Environmental factors

	P[environmental]
None	0.75
Waves	0.10
Wind	0.15

Load loss location

	P[environmental]
offshore supply vessel	0.15
main deck	0.85

Crane operation type

	P[environmental]
deck to deck	0.75
deck-vessel	0.25

Visual cues

Visual cues	P[visual cues|crane op type]	
	deck to deck crane operation	deck-vessel crane operation
line of site	0.75	0.65
no line of site	0.25	0.35

Conditional probabilities of loss of load control and loss of load

operating failure	rigging failure	visual cues	P[loss of control|oper fail, rig fail, vis cues]	P[loss of load|oper fail, rig fail, vis cues]
operate	operate	line of site	0.950	0.990
"	failure	"	0.600	0.850
failure	operate	"	0.700	0.850
"	failure	"	0.500	0.750
operate	operate	no line of site	0.900	0.9700
"	failure	"	0.500	0.500
failure	operate	"	0.700	0.500
"	failure	"	0.400	0.200

Casualty cost structure

operating failure	load	control	Loss value ($)
vessel	loss of load	loss of control	15,000.00
"	"	no control loss	50,000.00
"	no loss of load	loss of control	0.00
"	"	no control loss	10,000.00
deck	loss of load	loss of control	50,000.00
"	"	no control loss	100,000.00
"	no loss of load	loss of control	0.00
"	"	no control loss	50,000.00

Table 7.45: Human error probabilitites for offshore crane operation model: Company D

			P[human errors | crane operation type, visual cues, environ cues]						
crane op type	visual cues	environmental coditions	none	hum/syst interface	know/trn/ exper	mntl/phys lapse	violations	job design	comm/info
deck to deck	line of site	none	0.950	0.010	0.010	0.010	0.005	0.005	0.010
"	"	wind	0.850	0.050	0.030	0.010	0.010	0.010	0.040
"	"	waves	0.850	0.050	0.030	0.010	0.010	0.010	0.040
"	no line of site	none	0.900	0.030	0.020	0.010	0.005	0.015	0.020
"	"	wind	0.800	0.025	0.050	0.025	0.025	0.025	0.050
"	"	waves	0.800	0.025	0.050	0.025	0.025	0.025	0.050
vessel - deck	line of site	none	0.900	0.030	0.020	0.010	0.005	0.015	0.020
"	"	wind	0.800	0.025	0.050	0.025	0.025	0.025	0.050
"	"	waves	0.800	0.025	0.050	0.025	0.025	0.025	0.050
"	no line of site	none	0.800	0.050	0.040	0.015	0.020	0.025	0.050
"	"	wind	0.725	0.075	0.060	0.025	0.030	0.025	0.060
"	"	waves	0.725	0.075	0.060	0.025	0.030	0.025	0.060

		P[rig failure | human error, environmental factors, crane operation type]						
crane op type	environmental coditions	none	hum/syst interface	know/trn/ exper	mntl/phys lapse	violations	job design	comm/info
deck to deck	none	0.005	0.050	0.030	0.040	0.050	0.100	0.070
"	wind	0.050	0.060	0.050	0.060	0.070	0.120	0.090
"	waves	0.050	0.090	0.080	0.070	0.080	0.150	0.100
vessel - deck	none	0.005	0.070	0.090	0.070	0.075	0.150	0.150
"	wind	0.050	0.100	0.140	0.080	0.090	0.170	0.190
"	waves	0.200	0.090	0.120	0.090	0.100	0.180	0.190

		P[operating failure | human error, environmental factors, crane operation type						
visual cues	environmental coditions	none	hum/syst interface	know/trn/ exper	mntl/phys lapse	violations	job design	comm/info
deck to deck	none	0.005	0.050	0.030	0.040	0.050	0.100	0.070
"	wind	0.050	0.060	0.050	0.060	0.070	0.120	0.090
"	waves	0.050	0.090	0.080	0.070	0.080	0.150	0.100
vessel - deck	none	0.100	0.150	0.120	0.060	0.070	0.150	0.140
"	wind	0.150	0.200	0.150	0.090	0.100	0.200	0.180
"	waves	0.150	0.200	0.120	0.110	0.110	0.200	0.180

Table 7.46 - Evaluation of crane operations model

Event	EV[Event] ($)	SD[Event] ($)
Lost load	5,687	19,283

Event	P[Event]
Loss of load control	.082
Loss of load	.044

Human Error	P[human error| loss of load control]	P[human error| loss of load]
none	0.844	0.824
human system interface	0.042	0.037
knowledge-training-experience	0.033	0.030
mental-physical lapse	0.015	0.015
violation	0.013	0.012
job design	0.026	0.022
comm-info	0.047	0.040

7.5.4 HOE Management Alternatives -Camera Display Systems

Given the visual constraints that increase the risks of crane related casualties, Company D decided to study the alternative of installing cameras in areas that are outside of the line of sight of operators. With display monitors installed in the crane's cab, the operator would be have visual cues that would enable them to rely less upon platform personnel to communicate loading directions. It is estimated that the cost of a camera monitoring system for *Platform G* would be $200,000.

The implementation of the camera display system affects the incidence human errors and operating failures outside of the operators line of sight. Judgments are made as to the effects of the monitoring system on the probabilistic measurements of human error related contributors. These changes are reflected in Table 7.47 where more of the platform will become visually accessible to platform operators (visual cues). The addition of more visual cues will result in a reduction in the number of human system interface and communication-information errors which result in operating failure errors.

The results of implementing the camera monitoring system alternative are summarized in Table 7.48. Only marginal results are observed in the probabilities of the loss of load control and loss of load. However, a significant reduction in the incidence of load control losses and load losses as a result of both human system interface and communication-information errors are observed. The marginal results of the camera system alternative should lead Company D to evaluate other alternatives to complement the camera system (e.g. offshore safety vessel crew training to prevent rigging failures, fail-safe crane control systems for all cranes).

Table 7.47 - Changes in human error probabilities as a result of monitoring system - Company D

Visual cues

Visual cues	P[visual cues|crane op type]	
	deck to deck crane operation	deck-vessel crane operation
line of site	0.95	0.90
no line of site	0.05	0.10

Human errors

crane op type	visual cues	environmental conditions	P[human errors | crane operation type, visual cues, environ cues]		
			none	hum-syst interface	comm-info
deck to deck	no line of site	none	0.925	0.015	0.010
"	"	wind	0.833	0.025	0.025
"	"	waves	0.800	0.025	0.025
vessel-deck	"	none	0.845	0.030	0.025
"	"	wind	0.780	0.050	0.030
"	"	waves	0.780	0.050	0.030

Operating failures

visual cues	environmental conditions	P[operating failure | human error, environmental factors, crane operation type		
		hum-syst interface	violations	comm-info
deck to deck	none	0.020	0.050	0.030
"	wind	0.030	0.060	0.040
"	waves	0.040	0.045	0.050
vessel - deck	none	0.075	0.040	0.075
"	wind	0.090	0.060	0.090
"	waves	0.085	0.050	0.095

Table 7.48 - Evaluation of crane operations model

Event	EV[Event] ($) (% change w- monitor system)	SD[Event] ($)
Lost load	5,608	19,145

Event	P[Event] (% change w- monitor system)
Loss of load control	.070 (14%)
Loss of load	.040 (9%)

Human Error	P[human error| loss of load control] (%change w- monitor system)	P[human error| loss of load] (%change w- monitor system)
none	0.874 (3.5%)	0.860 (4.5%)
human system interface	0.028 (24.3%)	0.030 (28.5%)
knowledge-training-experience	0.026 (13.3%)	0.029 (12.1%)
mental-physical lapse	0.014 (6.7%)	0.015 (0.0%)
violation	0.010 (16.7%)	0.011 (15.4%)
job design	0.019 (13.6%)	0.023 (11.5%)
comm-info	0.029 (27.5%)	0.033 (29.8%)

7.6 SUMMARY

In this chapter two case study examples were presented to demonstrate the human error modeling procedures and quantitative measuring techniques. The *Exxon Valdez* and *Piper Alpha* disasters were chosen as the two case study examples as a result of the sufficient information in which to model the system failure and human related elements that contributed to the disasters. Influence diagram representations were constructed for each disaster. Influence diagram templates were developed from the diagram representations that preserved the primary causative factors to each disaster but did not maintain many of the unique casualty characteristics. For the *Exxon Valdez* model, a grounding and collision template was constructed and for the *Piper Alpha* disaster a simultaneous production and maintenance model was derived.

Quantitative measurements of the human errors characteristics related each disaster were derived using the *Human Error Safety Index Method.* These values were then input into the influence diagram templates to determine the overall risk index for grounding-collision and loss of fuel containment for the disasters.

Given the circumstances surrounding the *Exxon Valdez* and *Piper Alpha* disasters, both catastrophes may be deemed as "unacceptable" by both industry and societal standards. Though a catastrophe on the scale of *Exxon Valdez* had been cited as a once in 241 year event, it had occurred in just 12 years after operation [Davidson, 1990]. Similarly, the acceptable probability of offshore catastrophes on the scale of *Piper Alpha* had been considered acceptable with an annual probability of failure of 10^{-6}. *Piper Alpha* had also been operating for only 12 years before the disaster. The risks described are based upon historical data and experiences of those assessing and accepting the risks.

Given the existing state of data available, it is currently not possible to validate either model's risk index values. As mentioned in the Chapter 5, the strength of the quantitative modeling procedures described in this project report is the ability to update human error

related frequencies for both near misses and casualties and thus make more objective assessments of their impacts on marine casualties. Had these procedure been in place, the information would have been updated and the risk of the operations could have been assessed. It would have been determined prior to the disasters that the level of risk was unacceptable under the operating conditions specific to the *Exxon Valdez* tanker transit and *Piper Alpha* production-maintenance operations.

Trends in unsafe practices, policies, procedures, and organizational contributing factors could have led to the reduction of these risks through the instigation of HOE related management alternatives. The impact of HOE management alternatives on risk reduction have been assessed. A further description of identifying, modeling, and quantifying the impacts of HOE management alternatives for the grounding-collision and production-maintenance models were also provided. It is the intention that the information provided for these two disasters will provide a basis from which to begin for updating HOE related factors that lead to high consequence casualties.

A discussion was presented on the limiting factors of the current state of quantitative data to drive the models. The strength of the quantitative modeling procedures allow the user to update human error related data and thus enable users to formulate more objective models. If the updating procedure had been in place prior to the *Exxon Valdez* and *Piper Alpha* disasters, it is anticipated that primary HOE related factors that substantially increase the risk of these two catastrophes could have been identified.

Examples of evaluating techniques to assess the impacts of HOE management evaluation procedures were conducted. Two examples are described using heuristic judgments to model HOE management alternatives for the tanker grounding-collision and offshore production maintenance models. Alternative modeling techniques were exemplified. For the tanker grounding-collision model, changes in operational procedures were modeled by modifying the grounding-collision model template and accounting for the changes using the HESIM procedures. This was an example where explicit changes were made to the operation and were modeled directly by including the tug escort node. For the production-maintenance model, an alternatives to the gas detection and control program was evaluated by studying the impacts upon the human errors directly with no changes in the influence diagram model structure.

CHAPTER 8

CONCLUSIONS

8.1 SUMMARY

The objective of this research was to develop engineering reliability and decision analysis procedures and methodologies to identify, assess, and review alternatives to manage human and organizational errors (HOE) in the operations of tankers and offshore platforms. Five primary tasks were identified to reach this objective: (1) obtain well-documented case histories of tanker and offshore platform accidents whose causes are founded in HOE, (2) develop a classification framework for HOE, (3) analyze how HOE interactions caused the accidents, (4) investigate effectiveness and costs of various alternatives to reduce the incidence and effects of HOE, and (5) perform case history based evaluations of management alternatives.

As this research developed it was apparent that there are three major players in the human and organizational error reliability problem: (1) humans (individuals), (2) organizations (groups of individuals), and (3) systems (structures, equipment, and procedures). The second observation is that there are two approaches to the evaluation and management of human and organizational errors in improving reliability: qualitative and quantitative. Both of these approaches have benefits; the work indicates that they both should be mobilized to identify how and where to improve human and organizational error management. Qualitative modeling forms the basis from which to address the problem through operational procedures and regulation, and quantitative methods provide a means from which the procedures and regulations can be evaluated. One approach is not a substitute for the other.

The modeling of complex interactions between humans, organizations, and systems is not a simple problem. Currently, there is little definitive or information to assist in evaluating or analyzing these problems. The objective of the quantitative analysis developed in this report was not to produce numbers, it is to produce insights that can help improve the reliability of marine systems. The quantitative assessments should only be used as a decision support tool for qualitative judgments and are not a replacement for sound judgment and common sense. Modeling methodology is used as a framework from which to critically address the human element in reliability based analysis.

Chapter 2 described collection of accident reports and databases. Ninety written tanker and offshore casualty reports dated between 1979 and 1991 were collected in addition to 3 extensive casualty databases. Using this information, it was the intention to use the information in guiding the development of the human error classification and quantitative modeling. However, in this task, it became apparent that there was not any comprehensive, standardized, validated, commonly acceptable HOE classification documentation procedure or database.

In Chapter 3, an error classification that categorizes human, organizational, and human-system errors into 13 error types was described. Human and organizational errors were determined to be affected in a major way by commitments to safety and resources to achieve safety. The commitment to safety and resources affect the incidence of both organizational errors (top-level, middle, and front line management) and front-line

operator errors. Human and system errors were determined to be affected by environmental factors that can inhibit decisions and actions.

Chapter 4 described how post-mortem study models and examination of currently existing operations provide a basis on which to construct quantitative models (influence diagrams) of general classes of accidents. Study of past high consequence accidents can provide important insights into the complex interactions of humans, organizations, systems, and provide the basis for development of generic "templates" for evaluation of other similar systems. The influence diagram templates provide a basis in which to view the interactions of contributing factors to marine related casualties event though no quantitative assessments are made. However, the relative advantages and drawbacks should be addressed by the user. Knowledge and expertise of the operating system is particularly critical for studying current operations where accident data may be scarce.

The use of post-mortem study based models have both advantages and drawbacks. Post-mortems are extensive studies that can assist one in modeling cause-event based analysis, reveal latent errors, and allow for probabilistic updating. However, disadvantages should be noted in that they normally do not capture all critical interactions between the human and system. Casualty reports focus on attributing blame, focus on probability of failure of unique sets of circumstances, and are flawed by hindsight biases.

A four step approach was developed for using influence diagrams for post-mortem case study examples. To structure accident models, influence diagrams are first used as a tool to create representations that address critical interactions between the system and human operator for the marine disaster. Means by which to structure and update template models were proposed from the influence diagrams that retain critical causative mechanisms of the particular class of accident while not retaining the unique characteristics of the accident scenario. Templates are confirmed by comparing with disasters of that same particular class to determine if the template is consistent. Inconsistencies and uncertainties in the model can be developed in greater detail. A similar method was discussed for influence diagram model developments for existing operations.

A lack of quantitative information limits assessment of error probabilities and frequencies under various operating conditions. Because of a lack of definitive objective data to serve as input to such quantitative models, one must rely on expert opinion and information contained in existing accident reports and databases. In Chapter 5, quantification methods ranging from best heuristic judgments to a quantitative estimating procedure was developed. The *Human Error Safety Index Method* (HESIM), was introduced as a methodology for measuring the compounding impact on human and organizational errors resulting from accident solicitors (events, decisions, or actions).

The database system, the *Human and Organizational Error Data and Quantification System* (HOEDQS) serves two purposes. First, it provides a basis from which to obtain quantitative measurements for the HESIM described in the previous section. The HOEDQS allows the user to incorporate the data being collected and updated the expert judgment in generating quantitative measurements for organizational, human factors, system, and environmental contributors. Second, the database system provides a user friendly environment from which to generate probabilistic measures of human and organizational errors of marine casualties and near misses.

As data becomes available, a lesser reliance on expert opinion and judgment is required for the quantitative development and a greater reliance upon the data will lead to better quantitative measurements. The HOEDQS allows updating of human errors such that

there becomes a greater reliance upon objective data and less upon the judgmental indexing procedure. The strength of the data quantification system is that it is self correcting and has the capabilities of being updated and refined. The HESIM is used to assist in determining the impacts of organizational, system and task complexities, stress, routineness, and environmental conditions upon human errors and their effects upon increasing the risk. Error frequencies can be updated using the HESIM and HOEDQS and are then used to update the failure event index. The failure event risk index is then matched against the failure probabilities for that event. A functional relation between the risk index and probability of the accident event is then determined. This allows for forecasting the risk of failure events for future operations under various human operator conditions to determine if these operational conditions lead to an acceptable level of risk.

Chapter 6 addressed issues in determining HOE management alternatives. Human and organizational error management systems are required as a result of regulation or management operating policies. Once HOE management alternatives are identified, they are examined and evaluated to determine estimated impacts on the reduction of the frequency of the failures and the relative cost of implementation. Various modeling procedures were discussed by both explicitly and implicitly accounting for HOE management alternatives in modeling procedures. Factors to consider when determining "what is safe enough?" should be considered in the HOE management decision process.

In Chapter 7, 4 case studies were modeled to demonstrate HOE is to identified, assessed, and HOE management alternatives are evaluated. Post-mortem analyses entailed using well documented case studies (*Exxon Valdez* and *Piper Alpha*) as a basis from which to construct accident templates. Model templates were also constructed and analyzed for tanker loading-discharge operations and offshore crane operations using no post-mortem data. Both probability encoding and the HESIM were used as quantitative modeling techniques for the models. Human and organizational error management alternatives were modeled and evaluated.

8..2 OBSERVATIONS

The following summarizes the primary observations that were developed during this study:

There are three primary players in high consequence accidents: the front-line operators of the system (humans), the groups that are responsible for the management of the systems (organizations), and the physical elements (system).

High consequence accidents result from a multiplicity or compounding sequence of break-downs in the human, organization, and system; often there are "precursors" or early warning indications of the break-downs that are not recognized or are ignored.

Systems (physical components) are generally the easiest of the three components to address; design for human tolerances and capabilities (ergonomics), provision of redundancy and damage-defect tolerance, and effective early warning systems that provide adequate time and alarms so that systems can be brought under control are examples of potential measures. Error inducing systems are characterized by complexity, close coupling, latent flaws, small tolerances, severe demands, and false alarms.

Humans are more complex in that error states can be developed by a very wide series of individual characteristics and "states" including fatigue, negligence, ignorance, greed, folly, wishful thinking, mischief, laziness, excessive use of drugs, bad judgment, carelessness, physical limitations, boredom, and inadequate training. External (to the

system) and internal (in the system) environmental factors such as adverse weather, time of day, smoke, and temperature provide additional influences. Selection (determination of abilities to handle the job), training (particularly crisis management), licensing, discipline, verification and checking, and job design provide avenues to improve the performance of front-line operators.

While the human and system aspects are very important, the organization aspects frequently have over-riding influences. For instance, corporate "cultures" focused on production at the expense of quality, ineffective and stifled communications, ineffective commitment and resources provided to achieve quality, excessive time and profit pressures, conflicting corporate objectives, and counter-quality and integrity incentives are often present in "low reliability" organizations may over-ride human and systemic aspects. Generally, these aspects are the most difficult to address. Experience indicates that high reliability organizations tend to improve, while low reliability organizations do not improve rapidly, if at all.

The most important part of the HOE evaluation process is *qualitative*; a realistic and detailed understanding of the human, organization, and system aspects and potential interactions must underlie the entire process. Quantitative aspects provide an important framework from which to evaluate the potential effectiveness of proposed "fixes" and to examine the detailed interactions of human, organization, and system components.

There is no accepted and established marine system HOE database that can be relied upon to give accurate quantitative indications of the frequencies of accident contributors; in the case of specific accident scenarios, existing databases frequently give misleading indications of causes and consequences. Complex interactions are frequently not determined or lost in the reporting. Study of past high consequence accidents can provide important insights into the complex interactions of humans, organizations, and systems and can provide the basis for development of generic "templates" for evaluation of other similar systems. Study of "near misses" can show how potentially catastrophic sequences of actions and events can be interrupted and brought under control. There is no generally available database or archiving system for "near miss" information.

An adequate and understandable quantitative analysis system exists to assist evaluations of HOE; probability based "influence diagramming" has proven to be able to show the complex interactions and influences and efficiently produce quantitative indices that can indicate the effectiveness of alternative HOE "fixes." Because of the lack of accurate and definitive objective data to serve as input to such quantitative models, structured safety index models have been developed to allow encoding subjective judgment into the evaluation of probabilities. The HOEDQS format provides a structured framework from which complex interactions between events, environmental factors, system, task complexity, and HOEs may be examined. Still, to this date, there is no established methodology in practice to document casualties and near misses. Even the information that is currently being documented, excludes critical accident factors such as minor and major violations that lead to accident scenarios.

A reasonable and workable HOE classification system has been developed herein. This system should provide the basis for development of future marine operations accident reporting systems. Investigators need to be well trained in the evaluation of human and organization factors in marine accidents. An industry wide computer database system needs to be developed to improve the efficiency of accident reporting and analysis of results. Information on both accidents and "near misses" needs to be incorporated into this database.

The primary objective of HOE analyses should not be to produce numbers. The primary objective of HOE analyses should be to provide a disciplined and structured framework that is able to produce insights and information that can lead to improvements in the management of HOE. Even in the absence of reliable data, reliable quantitative assessments can be made. Judgments and experiences of operators, managers, regulators, and other decision makers are invaluable to the decision process. Quantitative measuring techniques for HOEs such as the HESIM can provide valuable quantitative insights. If consistent methodologies are used in quantitative measuring, reliable comparisons between HOE management alternatives can be assessed.

8.3 RECOMMENDATIONS FOR FUTURE DEVELOPMENTS

Given the current state of knowledge of identifying, assessing, and managing the impacts of human and organizational errors in operations of marine systems there are many areas of research that could greatly enhance the study of human and organizational errors in operations of marine systems. In general, modeling of human errors in operations of most technological systems have been task oriented in nature. Within the last few years, it has become apparent that management and organizational factors play a major role in both initiating and compounding of catastrophic accidents in marine systems.

One of the most critical areas for future developments is the implementation of an extensive database system to document the impacts of human errors at various stages of marine casualties. Since it has become commonly accepted that approximately 64% of all high consequence marine casualties are the result of human errors during operations, it is imperative that an extensive database system be implemented. Recent efforts by the USCG to train casualty investigators in identifying and properly documenting human and organizational errors for marine systems has been encouraging (Idaho National Engineering Laboratory, 1992). A critical area of deficiency has been in addressing the underlying root causes to accidents that are the results of organizational factors. Historically, casualty investigations have been focused more upon assessing blame than trying to get to the root causes of an accident scenario. Obligations to retain the information within the organization, legal reasons, and other factors limit the abilities to properly identify the root causes to human errors.

Another critical factor is the verification of model developments. Further refinements of the modeling procedures described in this project report is an iterative process. Updating of both quantitative measurements and modeling are critical to assuring the success of these modeling procedures. Bea and Roberts (1993) have initiated a research endeavor aimed at use and verification of the efforts described in this project report. This entails the study of loading and discharge operations for tankers. This is an extension of the work performed during this research. The initial background and template model for loading and discharge operations are presented in Chapter 7. Refinements and verification of these procedures will only help to enhance the use of these methods.

These methods should also be used to assess the impacts of HOE management alternatives. Modeling HOE related management alternatives have been discussed by Moore and Bea (1993). Chapter 6 discusses the use of HOE related management alternatives and risk assessment issues. An advantage of the modeling procedures discussed in this project report is that HOE management alternatives can be compared even with little or no available data. Using expert judgment comparisons can be made between alternatives to determine estimates of the degree of risk reduction that can be observed. These types of modeling procedures have been developed for both structural and fire and life safety factors for offshore platforms [Bea and Craig, 1993; Gale, 1993]. Further development of these procedures is a high priority.

REFERENCES

American Institute of Chemical Engineers. 1987. Dow's fire and explosion index hazard classification guide: 6th Edition. LC80-29237.

American Institute of Chemical Engineers. 1989. *Guidelines for Technical Management of Chemical Process Safety*. Center for Chemical Process Safety. American Institute of Chemical Engineers: New York.

American Nuclear Society and Institute of Electrical and Electronic Engineers. 1983. A guide to the performance of probabilistic risk assessments for nuclear power plants. NUREG/CR-2300. Vol. 1, 2.

Arrow, K. J. 1951. *Social Choice and Individual Values*. Cowles Foundation and Wiley: New York.

Arrow, K. J. 1972. *Decision and Organization*. North Holland Publications: Amsterdam, The Netherlands.

Ashley, D.B. 1992. Project risk identification using inference: Subjective expert assessment and historical data. Project Risk Management Class Notes. Department of Civil Engineering, University of California at Berkeley.

Bea, R.G. 1989. Human and organizational error in reliability of coastal and ocean structures. Proceedings, Civil College Eminent Overseas Speaker Program, Institution of Engineers, Australia.

Bea, R.G. 1990. *Reliability Based Design Criteria for Coastal and Ocean Structures*. National Committee on Coastal and Ocean Engineering. Institution of Engineers, Australia.

Bea, R.G., and Craig, M.J.K. 1993. Developments in the assessment and requalification of offshore platforms. *Proceedings of Offshore Technology Conference*: OTC 7138. Houston, TX.

Bea, R.G., and Moore, W.H. 1994. Reliability based evaluations of human and organizational errors in reassessment and requalification of platforms. Proceedings, *13th International Conference on Offshore Mechanics and Arctic Engineering: Safety and Reliability Symposium*. American Society of Mechanical Engineers. Houston, TX.

Bea, R.G., and Moore, W.H. 1993. Operational reliability and marine systems. *New Challenges to Understanding Organizations*. K.H. Roberts (ed.). Macmillan: New York. pp. 199-229.

Bea, R.G., and Roberts, K.H. 1993. California Sea Grant proposal for Tanker Load and Discharge Study. Department of Naval Architecture and Offshore Engineering, University of California at Berkeley.

Bekkevold, E., Fagerjord, O., Berge, M., and Funnemark, E. 1990. Offshore accidents, do we ever learn? A 20 years report from Veritec's World Wide Offshore Accident Databank (WOAD). *Offshore Safety Conference*. Brazil.

Bell, B.J., and Swain, A.D. 1983. A procedure for conducting a human reliability analysis for nuclear power plants. *NUREG-/CR-2254*. Report by Sandia National Laboratories to Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission.

Bello, G.C., and Colombari, V. 1980. Empirical technique to estimate operator's errors (TESEO). *Reliability Engineering*. Vol. 1, No. 3.

Bertrand, A. and Escoffier, L. (No date.) IFP databanks on offshore accidents. Division of Planning and Information. Institut Français du Pétrole. Rueil-Malmaison Cedex, France.

Bodily, S.E. 1985. *Modern decision making: A guide to modeling with decision support systems*. McGraw Hill, Inc.

Brown C. B., and Yin., X/ 1988. Errors in structural engineering. *Journal of Structural Engineering*, Vol. 114, No. 11. pp. 2575- 2593.

California State Lands Commission. 1992. Personal communications.

CASMAIN. 1991. USCG casualty database. 1981-1990.

Carson, W.G. 1982. *The Other Price of Britain's Oil: Safety and Control in the North Sea*. Martin Robertson and Company Ltd.: Oxford, England.

Comer, M.K., Seaver, D.A., Stillwell, W.G., and Gaddy, C.D. 1984. General human reliability estimates using expert judgment. *NUREG/CR-3688*. Vol. 1 and 2. Washington, D.C. Nuclear Regulatory Commission.

Construction Industry Research and Information Association. 1977. Rationalization of safety and serviceability factors in structural codes. London, England: CIRIA Report No. 63.

Connaughton, S.T. 1990. Vessel pollution prevention and response considerations. *New Oil Pollution Act of 1990 Conference*. Government Institutes, Inc.

Danenberger, E.P. and Schneider, P.R. 1991. *Piper Alpha* - the US regulatory response. Proceedings, *Offshore Operations Post Piper Alpha Conference*. London.

Davidson, A. 1990. *In Wake of the Exxon Valdez: The Devastating Impact of the Alaska Oil Spill*. Sierra Club Books: San Francisco, CA.

Decision Focus Incorporated. 1991. Professional Edition of InDia™: Users Guide. Version 2.0. Decison Focus Incorporated. Los Altos, CA.

Det Norske Veritas. 1991. Comparative study on potential oil spill in collision and/or grounding - different tanker designs. *Tanker Spills: Prevention by Design*. Appendix F. Committee on Tank Vessel Design, Marine Board Commission on Engineering and Technical Systems. National Academy Press: Washington, D.C.

Dougherty, E.M., Jr., and Fragola, J.R. 1986. *Human Reliability Analysis*. John Wiley and Sons: Brisbane, Australia.

Dynamic Research Corporation Man-Machine Systems Department 1989. *The Role of Human Factors in Marine Casualties* (Final Report). Prepared for the U.S. Coast Guard. Contract no.: N00024-D-4373.

Flint, A.R., and Baker, M.J. 1976. Risk analysis for offshore structures: The aims and methods, design and construction of offshore structures. Instiute of Civil Engineers. London.

Freudenburg, W.R. 1988. Perceived risk, real risk: Social science and the art of probabilistic risk assessment. *Science*, Vol. 242.

Gale, W.E. 1993. *Fire and Life Safety Assessment and Indexing Method.* Doctor of Philosophy Dissertation. School of Engineering. University of California at Berkeley.

Haney, L.N., Blackman, H.S., Bell, B.J., Rose, S.E. Hesse, L.A., and Jenkins, J.P. 1989. Comparison and application of quantiative human reliabilty analysis methods for the Risk Methods Integration and Evaluation Program (RMIEP). *NUREG/CR-4835*, U.S. Nuclear Regulatory Commission, Washington, D. C.

Hannaman, G.W., Sprugin, A.J., and Lukic, Y.D. 1984. Human cognitive reliability model for PRA analysis. NUS-4531. Electrical Power Research Institute: Palo Alto, CA.

Heising, C.D., and Grenzebach, W.S. 1989. The *Ocean Ranger* oil rig disaster: A risk analysis. *Risk Analysis*. Vol. 9, No. 1.

Henley, E.J., and H. Kumamoto. 1981. *Reliability Engineering and Risk Assessment.* Englewood Cliffs, N.J.: Prentice Hall Inc. Cambridge, U.K.: Cambridge University Press.

Howard, R. A. 1966. Information value theory. *IEEE Transactions on Systems, Man, and Cybernetics*. Vol. SSC-2 (1). pp. 22-26.

Howard, R.A. 1990. From influence to relevance to knowledge. From *Influence Diagrams, Belief Nets and Decision Analysis*. M.R. Oliver and J.Q. Smith (Eds.). Wiley and Sons: New York. pp. 3-24.

Howard, R.A., and Matheson, J.E. 1981. Influence diagrams. *The principles and applications of decision analysis*. Vol. II. R.A. Howard and J.E. Matheson (Eds.). Strategic Decisions Group: Menlo Park, CA.

Idaho National Engineering Laboratory. 1992. Instruction notes for a human factors module for the United States Coast Guard Investigative Department Course. Prepared for the U.S. Coast Guard Research and Development Center. Groton, CT.

Imperial Chemical Industries. 1980. Technical manual for Mond fire, explosion and toxicity index. Mond Division Technical Department, Winnington Laboratory.

Ingles, O.G. 1985. *Human Error and Its Role in the Philosophy of Engineering*. Doctoral Thesis. University of New South Wales, Australia.

Kahneman, D., Slovic P., and Tversky, A. 1982. *Judgment Under Uncertainty: Heuristics and Biases*. Cambridge University Press: New York.

Keeble, J. 1991. *Out of the Channel: The Exxon Valdez Oil Spill in Prince William Sound.* HarperCollins Publishers: New York.

Koch, B.A. 1993. Differentiating reliability seeking organizations from other organizations: Development and validation of assessment devices. *New Challenges to Understanding Organizations*. K.H. Roberts (ed.). Macmillan: New York. pp. 75-98.

Kuprenas, J.A. 1988. Use of influence diagrams to assess the cost and schedule impact of constuction changes. Dr. Engineering Dissertation. Department of Civil Engineering, Construction Engineering and Management. University of California at Berkeley.

La Porte, T.R. 1988. High reliability organization project. University of California at Berkeley.

Laroque, G.R., and Mudan, K.S. 1982. Cost and benefits of OCS regulations: Vol. 3 - Preliminary risk analysis of outer continental shelf activities. Arthur D. Little, Inc. Cambridge, MA.

March, J. G., and Simon, H.A. 1958. *Organizations*. John Wiley and Sons: New York.

Marton, T., and Purtell, T.W. 1990. Investigations in the role of human factors in man related marine casualties. U.S.Coast Guard Internal Report.

McNamee, P., and Celona, J. 1990. *Decision Analysis with Supertree*. Scientific Press: San Francisco, CA.

Melchers, R.E. 1987. *Structural Reliability Analysis And Prediction*. Ellis Horwood Limited, Halsted Press: a division of John Wiley and Sons: Brisbane, Australia.

Minerals Management Service. 1984. *Risk Analysis of Crane Accidents*. OCS Report MMS 84-0056.

Minerals Management Service. 1984. *Risk Analysis of Welding Accidents*. OCS Report MMS 84-0064.

Minerals Management Service. 1988. *Accidents Associated With Oil and Gas Operations: Outer Continental Shelf 1956-1986*. OCS Report MMS 88-0011.

Moan, T. 1983. *Safety of offshore structures*. Proceedings, Fourth International Conference on Applications of Statistics and Probability in Soil and Structural Engineering.

Moore, W.H. 1994. The grounding of *Exxon Valdez*: An examination of the human and organizational factors. *Marine Technology*. Society of Naval Architects and Marine Engineers. Vol. 31, No. 1.

Moore, W.H. 1993. Management of Human and Organizational Error in Operations of Marine Systems. Doctor of Engineering Dissertation. Department of Naval Architecture and Offshore Engineering, University of California at Berkeley.

Moore, W.H. 1991. Human and organizational error in marine systems: A review of existing taxonomies and databases. Research Report No. HOE-91-1, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering*, University of California at Berkeley.

Moore, W.H., Bea, R.G., and Roberts, K.H. 1993. Improving management of human and organizational errors in tanker operations. Proceedings of *Society of Naval Architects and Marine Engineers - Ship Structure Symposium '93*, Arlington, VA.

Mulhbauer, W.K. 1992. *Pipeline Risk Management Manual.* Gulf Publishing Company: Houston, TX.

National Research Council. 1991. Tanker spills: Prevention by design. Committee on Tank Vessel Design, Marine Board Commission on Engineering and Technical Systems. National Academy Press: Washington, D.C.

National Research Council. 1981. Reducing tankbarge pollution. National Academy Press: Washington, D.C.

Nelson, H.E., and Shibe, A.J. 1978. A system for fire safety evaluation of health care facilities. Center for Fire Research, National Bureau of Standards. NBSIR 78-1555.

Nessim, M.A., and Jordaan, I.J. 1985. Models for human error reliability. *Journal of Structural Eng.* Vol. 111, No 6.

Nowak, A.S. 1986. Modeling human error in structural design and construction. Proceedings of a Workshop Sponsored by the National Science Foundation, American Society of Civil Engineers.

Offshore Certification Bureau. 1988. Comparative safety evaluation of arrangements for accommodating personnel offshore. Report OTN-88-175.

Oliver, R.M., and Yang, H.J. 1990. Baysian updating of event tree parameters to predict high risk incidents. From *Influence Diagrams, Belief Nets and Decision Analysis.* Oliver, M.R. and Smith (Eds.), J.Q. Wiley and Sons: New York. pp. 277-296.

Panel on Human Error in Merchant Marine Safety. 1976. Human error in merchant marine safety. Maritime Transportation Research Board, National Academy of Sciences, Washington, D.C.

Paté-Cornell M.E. 1992. A post-mortem analysis of the *Piper Alpha* accident: Technical and organizational factors. Research Report No. 92-2, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering*, University of California at Berkeley.

Paté-Cornell, M. E. 1986. Warning systems in risk management. *Risk Analysis.* Vol. 6, No. 2.

Paté-Cornell, M. E., and Seawell, J.P. 1988. Engineering reliability: The organizational link. Proceedings of the ASCE Specialty Conference on Probabilistic Mechanics and Structural and Geotechnical Safety. Blacksburg, VA.

Paté-Cornell, M. E., and Bea, R.G. 1989. Organizational aspects of reliability management: Design, construction, and operation of offshore platforms. Research Report No. 89-1, Department of Industrial Engineering and Engineering Management, Stanford University.

Perrow, C. 1984. *Normal Accidents: Living with High Risk Technologies.* Basic Books, Inc.: New York.

Phillips, L.D., Humphreys, D.E., and Selby, D.L. 1990. A socio-technical approach to assessing human reliability. From *Influence Diagrams, Belief Nets and Decision Analysis*. M.R. Oliver and J.Q. Smith (Eds.). Wiley and Sons: New York. 1990. pp. 253-276.

Potash, L.M., Stewart, M., Dietz, P.E., Lewis, C.M., and Dougherty Jr., E.M. 1981. Experience in integrating the operator contributions in the PRA of actual operating plants. *ANS/ENS Topical Meetng on Probabilistic Risk Assessment.* American Nuclear Society. Port Chester, N.Y.

Reason, J. 1990. *Human Error.* Cambridge University Press: New York.

Reason, J. 1992. How to promote error tolerance in complex systems in the context of ships and aircraft.

Reid, S.G. 1989. Guidelines for risk based decision-making. Investigation Report NO. S726, The University of Sydney School of Civil and Mining Engineering.

Report of the Royal Commission on the *Ocean Ranger* Marine Disaster. 1985. Ottawa, Ontario, Canada.

Roberts, K.H., and Moore, W.H. 1992. The Gordian Knot: Into which sailed the *Exxon Valdez.* Research Report No. 92-1, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering, University of California, Berkeley.*

Royal Norwegian Council for Scientific and Industrial Research. 1979. Risk assessment report of the Norwegian offshore petroleum activities. Oslo, Norway.

Shachter, R.D. 1986. Evaluating influence diagrams. *Operations Research.* Vol. 34, No. 6.

Siktec. 1986. Fatality risk offshore. Internal report. Trondheim, Norway.

Spetzler, C.S., and Staël von Holstein, C-A.S. 1972. Probability encoding in decision analysis. Paper presented at the ORSA-TIMS-AIEE 1972 Joint National Meeting, Atlantic City, N.J.

Stahl, B. 1986. Reliability engineering and risk analysis. *Planning and Design of Fixed Offshore Platforms.* Van Nostrand Reinhold Company: Melbourne, Austrailia.

Swain, A.D. 1986. Accident sequence evaluation program: Human reliability analysis procedures. *NUREG/CR-4772.* U.S. Nuclear Regulatory Commission, Washington, D.C.

Swain, A. D., and Guttmann, H. E. 1983. Handbook of human reliability analysis with emphasis on nuclear power plant applications: Final Report, *NUREG/CR-1278*, U.S. Nuclear Regulatory Commission, Washington, D. C.

Swain, A.D. and Weston, L.M. An approach to the diagnosis and misdiagnosis of abnormal conditions in post-accident sequences in complex man-machine systems. In L. Goldstein, H. Anderson, and S. Olson (Eds.), *Tasks, Errors, and Mental Models.* Taylor and Francis: London.

Swaton, E., and Tolstkh, V. 1990. Human factor insights from international event reports. Proceedings, *U. S. Nuclear Regulatory Commission Eighteenth Water Reactor Safety Information Meeting*. Rockville, Maryland. NUREG/CP0114. Vol. 1. pp. 221-233.

United Kingdom Department of Energy. 1988a. *Piper Alpha Technical Investigation: Interim Report.* (Petrie Report) Crown: London.

United Kingdom Department of Energy. 1988b. *Piper Alpha Technical Investigation: Further Report.* (Petrie Report) Crown: London.

United Kingdom Department of Energy. 1990. *The Public Inquiry into the Piper Alpha Disaster*, The Hon Lord Cullen, Vol. 1, 2. HMSO Publications: London.

U.S. Department of Commerce, National Bureau of Standards. 1985. Application of risk analysis to offshore oil and gas operations. Proceedings, *International Workshop, NSB Special Publications 695*, Washington, D.C.

U.S. Department of Interior, Minerals Management Service. 1984. *Risk Analysis of Crane Accidents*. OCS Report MMS 84-0056.

U.S. Reactor Safety Study. 1975. *An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*. WASH-1400.

Veritas Offshore Technology Service A/S. 1989. *Piper Bravo* pre-development: Safety evaluation - PQ (Floater) alternative. Prepared for Brown and Root Vickers, Ltd. Veritec Report No. 89-3139.

Veritec. 1988. The Worldwide Offshore Accident Data Bank (WOAD). Annual Reports through 1988. Oslo, Norway.

Vinnem, J.E., and Hope, B. 1986. *Offshore Safety Management*. Tapir Publishers: Trondheim, Norway.

Wenk, E., Jr. 1986. *Tradeoffs, Imperatives of Choice in a High-tech World.* The Johns Hopkins University Press: Baltimore, MD.

Weick, K.E. 1987. Organizational culture as a source of high reliability. *California Management Review.*

Zion Probabilisitic Safety Study. 1981. Commonwealth Edison Company. Chicago, IL.

APPENDIX 1

Related Human and Organizational Error References

Barnett, M. 1991. *LICOS*- A liquid cargo operations simulator and its use in training for the handling of potential emergencies. Proceedings, *Human Factors in Offshore Safety Conference*. Aberdeen, Scotland.

Bea, R.G., Paté-Cornell, M.E. 1989. *Organizational Aspects of Reliability Management: Design, Construction, and Operations of Offshore Platforms*. Research Report No. 89-1, Department of Industrial Engineering and Engineering Management, Stanford University.

Bea, R. G., and Moore, W. H. 1991. Management of human and organizational error in operational reliability of marine structures. *Proceedings, 2nd SNAME Offshore Symposium: Design Criteria and Codes*. Houston, TX.

Bekkevold, E., Fagerjord, O., Berge, M., and Funnemark, E. 1990. Offshore accidents, do we ever learn? A 20 years report from VERITEC's World Wide Offshore Accidente Databank (WOAD). *Offshore Safety Conference*. Brazil.

Cole, M.W., Marucci, T.F., and Taft, D.G. 1987. MODU marine safety: Structural inspection and readiness surveys. *Journal of Petroleum Technology*.

Drager, K.H. 1979. Cause relationships of collisions and groundings. Det Norske Vertitas.

Dyer-Smith, M. 1991 Apocalypse soon: Should the world-wide decline in skilled maritime labor concern the offshore oil industry? Proceedings, *Human Factors in Offshore Safety Conference*. Aberdeen, Scotland.

Dynamic Research Corporation. 1992. Role of human factors in marine casualties. Final report prepared for the U.S. Coast Guard. Contract number N00024-85-D-4373.

Embrey, D. 1991. Managing Human Error in the Offshore Oil and Gas Industries. Proceedings, *Human Factors in Offshore Safety Conference*. Aberdeen, Scotland.

Fitzgerald, B.P., Grant, M.Mc.D., and Green, M.D. 1991. A practical methodology for risk assessment of offshore installations. *Proceedings, Offshore Operations Post Piper Alpha Conference*. London.

Fouchee, H.C., and Helmreich, R.L. 1988. Group interaction and flight crew performance. *Human Factors in Aviation.* E.L. Weiner and D.C. Nagel (ed.), Academic Press, Inc.: San Diego, CA.

Hallas, O. 1991. A model for human error prevention in design- experiences from an offshore project. Proceedings, *Human Factors in Offshore Safety Conference*, Aberdeen, Scotland.

Hashemi, K. 1991. An integrated approach to a safety case. Proceedings, *Human Factors in Offshore Safety Conference.* Aberdeen, Scotland.

Hutchins, E. 1991. Organizational work by adaptation. *Organizational Science.* Vol. 2, No. 1.

Ingstad, O. 1991. Approaching better human factors design of offshore control rooms. Proceedings, *Human Factors in Offshore Safety Conference.* Aberdeen, Scotland.

Kontogiannis, T. 1991. Decision making under high stress: An evaluation of models of stress, case studies, and countermeasures. Proceedings, *Human Factors in Offshore Safety Conference.* Aberdeen, Scotland.

Kosmowski, K.T., and Duzinkiewicz, K. 1992. An integrated approach in probabilistic modeling of hazardous technological systems with emphasis on human factors.

Lynagh, N. 1991 The impact of weather forecasting on offshore safety. *Proceedings, Offshore Operations Post Piper Alpha Conference.* London, February.

Lynagh, N., and Morgan, S. K. 1991. Environmental design criteria for transporting offshore oil platforms through areas affected by tropical cyclones. Proceedings, *Society of Naval Architects and Marine Engineers 2nd Offshore Symposium: Design and Codes,* Houston TX.

Madsen, H.O., Krenik, S., and Lind, N.C. 1986. *Methods of Structural Safety.* Prentice-Hall Inc. Englewood Cliffs, N.J.

Martin, T. 1991. Human response in an emergency situation: A review of actions during the *Piper Alpha* disaster. Proceedings, *Human Factors in Offshore Safety Conference.* Aberdeen, Scotland.

Matousek, M. 1977. Outcomings of a survey on 800 construction failures. *IABSE* Colloquium on Inspection on Quality Control: Cambridge, England.

Melchers, R. E. 1980. Societal options for assurance of structural performance. *Final Report, 11 Congress.* IABSE, London.

Miller, G.E. 1991. Human Factors Engineering (HFE): Review of *Auger* cranes. Report for *Shell Offshore Inc.*, Deepwater Division.

Miller, G.E. 1990 The omission of human engineering in the design of offshore equipment and facilities: How come? Proceedings, *Offshore Technology Conference.* Houston, TX.

Moan, T. 1981. The *Alexander Kielland* accident. Report of the Norwegian Government Commission.

Moore, W.H., and Bea, R.G. 1993. Human and organizational errors in operations of marine systems: *Occidental Piper Alpha.* Proceedings, *12th International Conference on Offshore Mechanics and Arctic Engineering*. Glasgow, Scotland.

Moore, W.H., and Bea, R.G. 1993. Human and organizational errors in operations of marine systems: *Occidental Piper Alpha* and high pressure gas systems on offshore platforms. Proceedings, *Offshore Technology Conference*. Houston, TX. OTC 7121.

Moore, W.H., and Bea, R.G. 1992. Modeling human errors in operations of marine systems: Case study examples. Research Report No. HOE-92-5, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering*, University of California at Berkeley.

Moore, W.H., and Bea, R.G. 1992. Modeling the effects of human errors from post-mortem marine casualty studies. Research Report No. HOE-92-4, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering*, University of California at Berkeley.

Moore, W.H., and Bea, R.G. 1992. A practical human error taxonomy for marine related casualties. Research Report No. HOE-92-3, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering*, University of California at Berkeley.

Nagel, D.C. 1988. Group interaction and flight crew performance. *Human Factors in Aviation*. E.L. Weiner and D.C. Nagel (eds.). Academic Press, Inc.: San Diego, CA.

National Research Council Marine Board. 1990. *Crew Size and Maritime Safety*. National Academy Press: Washington, D. C.

Netland, K., The human in a centralized control environment for drilling. Proceedings, *Human Factors in Offshore Safety Conference*. Aberdeen, Scotland.

Noreng, Ø. 1980. *The Oil Industry and Government Strategy in the North Sea*. Croom Helm: London.

Offshore Certification Bureau. 1988. Comparative safety evaluation of arrangements for Oljedirektoratet - Norwegian Petroleum Directorate. 1990. Regulations concerning implementation and use of risk analyses in the petroleum activities with guidelines.

Paté-Cornell, M.E. 1990. Organizational aspects of engineering system safety: The case of offshore platforms. *Science*, Vol. 250.

Pollard, J.K., Stearns, M., and Sussman, E.D. 1990. Shipboard crew fatigue, safety, and reduced manning. Final Draft Report Prepared by U.S. Department of Transportation, Transportation Systems Center, Cambridge, MA.

Rasmussen, J., 1986. *Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering*. Series Vol. 12. Elsevier North Holland Inc.: New York.

Roberts, K. H. 1989. New challenges in organizational research: high reliability organizations. *Industrial Crisis Quarterly* 3. Elsevier Science Publishers B.V.: Amsterdam, Netherlands. pp. 111-125.

Roberts, K.H. 1990. *Top management and effective leadership in high technology.* L. Gomez-Mehia and M. W. Lawless (eds.). Research series on managing the high technology firm. Vol. III. JAI Press: Greenwich, CT.

Roberts K.H., and Moore, W.H. 1993. Bligh Reef dead ahead: The grounding of the *Exxon Valdez. New Challenges to Understanding Organizations.* K.H. Roberts (ed.). Macmillan: New York. pp. 231-249.

Robinson, P. 1991. Safety performance and organizational culture: an organization perspective. Proceedings, *Human Factors in Offshore Safety Conference.* Aberdeen, Scotland.

Roggeveen, V. 1991. Controlling the human factor in offshore industry safety. Proceedings, *Human Factors in Offshore Safety Conference.* Aberdeen, Scotland.

Rouse, W.B. 1980. *Systems Engineering Models of Human Machine-Interaction,* Series Vol. 6. Elsevier North Holland Inc.: New York.

Salvendy, G. (ed.) 1987. Human error and human reliability: Handbook of human factors. John Wiley and Sons: New York.

Sharples, B.P.M. 1990. oil pollution by the offshore industry contrasted with tankers: An examination of the facts. Paper presented at the Institution of Mechanical Engineers, London, England.

Stinchcombe, A.L., and Heimer, C.A. 1985. *Organizational theory and project management: Administering uncertainty in Norwegian offshore oil.* Norwegian University Press: Oslo, Norway.

Sutherland, V.J. 1991. Human factors in accident involvement offshore. Proceedings, *Human Factors in Offshore Safety Conference.* Aberdeen, Scotland.

Sylvester-Evans, R. 1991. Management and organizational failings leading to major accidents. Proceedings, *Human Factors in Offshore Safety Conference.* Aberdeen, Scotland.

Taft, D.G., Carroll K.L., Major, R.A. and Marucci, T.F. 1986. Conducting effective drills on MODU's. Proceedings, *1986 IADC/SPE Drilling Conference.* Dallas, TX.

Waldram, I. 1991. Contractor Safety audits: the inclusion of human factors. Proceedings, *Human Factors in Offshore Safety Conference.* Aberdeen, Scotland.

APPENDIX 2

Casualty Data Catalog

NATIONAL TRANSPORTATION SAFETY BOARD

National Transportation Safety Board/U.S. Coast Guard. 1976. *SS C.V. Sea Witch - SS Sesso Brussels (Belgium); Collision and Fire in the New York Harbor on 2 June 1973 with Loss of Life.* Report no. USCG/NTSB MAR-75-6.

National Transportation Safety Board/United States Coast Guard. 1977. *SS Key Trader and SS Baune (Norwegian); Collision in the Mississippi River on 18 January 1974 with Loss of Life.* Report no. USCG/NTSB MAR-77-1.

National Transportation Safety Board/United States Coast Guard. 1977. *SS Edgar M. Queeny - S/T Corinthos; Collision at Marcus Hook, Pensylvania on 31 January 1975 with Loss of Life.* Report no. USCG/NTSB MAR-77-2.

National Transportation Safety Board. 1980. *Collision of the S/T Texaco Iowa and the M/T Burmah Spar on the Mississippi River, Pilottown, Louisiana, October 3, 1978.* NTSB/MAR-80-3.

National Transportation Safety Board. 1980. *Collision of Peruvian Freighter M/V Inca Tupac Yupanqui and U.S. Butane Barge Panama City, Good Hope, Louisiana, August 30, 1979.* PB80-200850, NTSB-MAR-80-7.

National Transportation Safety Board. 1980. *Collision of S/T Mobil Vigilant and S/T Marine Duval on the Neches River Near Beaumont, Texas, February 25, 1979.* NTSB/MAR-80-8.

National Transportation Safety Board. 1980. *Collision of United States Tankship S.S. Exxon Chester and Liberian Freighter M.V. Regal Sword in the Atlantic Ocean Near Cape Cod, Massachusetts, June 18, 1979.* NTSB/MAR-80-11.

National Transportation Safety Board. 1980. *Liberian Tank Vessel M/V Seatiger Explosion and Fire, Sun Oil Terminal, Nederland, Texas, April 19, 1979.* NTSB/MAR-80-12.

National Transportation Safety Board. 1980. *Collision of U.S. Coast Guard Cutter Blackthorn, and U.S. Tankship Capricorn, Tamapa Bay, Florida, January 28, 1980.* NTSB/MAR-80-14.

National Transportation Safety Board. 1980. *Collision of Liberian Tankship M/V Pina and the Towboat Mr. Pete and Its Tow Mile 99.3, Lower Mississippi River, December 19, 1979.* NTSB/MAR-80-17.

National Transportation Safety Board. 1980. *Explosion and Fire on Board the SS Chevron Hawaii with Damages to Barges and to the Dear Park Shell Oil Company Terminal, Houston Ship Channel, September 1, 1979.* NTSB/MAR-80-18.

National Transportation Safety Board. 1981. *U. S. Tankship S/S Texaco North Dakota and Artificial Island IE-361-A, Collision and Fire, Gulf of Mexico, August 21, 1980.* PB81-191371, NTSB/MAR-81-4.

National Transportation Safety Board. 1981. *Collision of the U.S. Mississippi River Steamer Natchez and U.S. Tankship SS Exxon Baltimore, New Orleans, Louisiana, March 29, 1980.* PB81-231797, NTSB/MAR-81/5.

National Transportation Safety Board. 1981. *Grounding of the U.S. Tankship S.S. Concho Constable Hook, Reach of Kill Van Kull, Upper New York Harbor, January 19, 1981.* PB81-249443, NTSB/MAR-81-11.

National Transportation Safety Board. 1981. *Liberian Chemical Tankship M/V Coastal Transport Collision with U.S. Offshore Supply Vessel M/V Sallee P., Lower Mississippi River near Venice, Louisiana, November 24, 1980.* PB82-105016, NTSB/MAR-81-12.

National Transportation Safety Board. 1981. *Explosion and Fire on Board the U.S. Tankship Monticello Vicotry, Port Arthur Texas, May 31, 1981.* PB82-157165, NTSB/MAR-81-14.

National Transportation Safety Board. 1982. *Collision of the U.S. Tankship Pisces with the Greek Bulk Carrier Trademaster, Mile 124, Lower Mississippi River, December 27, 1980.* PB82-916402, NTSB/MAR-82-2.

National Transportation Safety Board. 1982. *Sinking of the M/V Oxy Producer in the Atlantic Ocean Near the Azores Island September 20, 1981.* PB82-916406, NTSB/MAR-82-6.

National Transportation Safety Board. 1983. *Capsizing and Sinking of the U.S. Mobile Offshore Drilling Unit Ocean Ranger Off the East Coast of Canada 166 Nautical Miles East of St. John's, Newfoundland February 15, 1982.* NTSB/MAR-83/2.

National Transportation Safety Board. 1983. *Explosion and Fire Onboard U.S. Coastal Tankship Poling Bros. No. 9, East River, New York Harbor, February 26, 1982.* PB83-916403, NTSB/MAR-83/03.

National Transportation Safety Board. 1983. *Collision of the U.S. Towboat Creole Genii and Liberian Tank Vessel Arkas Near Mile 130 Mississippi River, March 31, 1982.* PB83-916404, NTSB/MAR-83/04.

National Transportation Safety Board. 1983. *Breakaway of 38 Barges, Arkansas River, December 4, 1982.* PB83-916405, NTSB/MAR-83/05.

National Transportation Safety Board. 1983. *Engineroom Flooding and Near Foundering of U.S. Tankship Ogden Willamette, Caribbean Sea, June 16, 1982.* PB83-916406, NTSB/MAR-83/06.

National Transportation Safety Board. 1983. *Explosion and Fire Onboard the U.S. Tankship Golden Dolphin in the Atlantic Ocean, March 6, 1982.* PB83-916407, NTSB/MAR-83/07.

National Transportation Safety Board. 1984. *Collision of the U.S. Coast Guard Cutter Polar Sea and Barges, Seattle Washington, September 10, 1983.* PB84-916403, NTSB/MAR-84/03.

National Transportation Safety Board. 1984. *Capsizing and Sinking of the United States Drillship Glomar Java Sea in the South China Sea 65 Nautical Miles South-Southwest of Hainan Island, Peoples Republic of China, October 25, 1983.* NTSB/MAR-84/08.

National Transportation Safety Board. 1984. *Grounding of United States Tankship Mobil Oil, in the Columbia River near Saint Helens, Oregon, March 19, 1984.* PB84-916409, NTSB/MAR-84/09.

National Transportation Safety Board. 1985. *Explosion and Sinking of the United States Tankship SS American Eagle Gulf Mexico, February 26 and 27, 1984.* PB85-916406, NTSB/MAR-85/06.

National Transportation Safety Board. 1986. *Explosion and Fire Aboard the U.S. Mobile Offshore Drilling Unit Zapata Lexington, Gulf of Mexico, September 14, 1984.* PB85-916412, NTSB/MAR-85/12.

National Transportation Safety Board. 1986. *Explosion and Fire Onboard the U.S. Mobile Offshore Drilling Unit Glomar Arctic II in the North Sea, 130 Nautical Miles East-Southeast of Aberdeen, Scotland, January 15, 1985.* PB86-916403, NTSB/MAR-86/03.

National Transportation Safety Board. 1986. *Explosions and Fire On Board U.S. Chemical Tankship Puerto Rican in the Pacific Ocean Near San Francisco, California, October 31, 1884.* PB86-916405, NTSB/MAR-86/05.

National Transportation Safety Board. 1986. *Collapse of the U.S. Mobile Offshore Drilling Unit Penrod 61, Gulf of Mexico, October 27, 1985.* PB86-916411, NTSB/MAR-86/10.

National Transportation Safety Board. 1987. *Capsizing and Sinking of the United States Drillship Glomar Java Sea in the South China Sea 65 Nautical Miles South-Southwest of Hainan Island, Peoples Republic of China, October 25, 1983.* NTSB/MAR-87/02.

National Transportation Safety Board. 1987. *Explosion Aboard the U.S. Tank Barge TTT 103, Pascagoula, Mississippi, July 31, 1986.* PB87-916405, NTSB/MAR-87/05.

National Transportation Safety Board. 1987. *Engineroom Flooding of the U.S. Tankship Prince William Sound Near Puerto Vallarta, Mexico, May 1986.* PB87-916406, NTSB/MAR-87/07.

National Transportation Safety Board. 1987. *Fires On Board the Panamanian Tank Ship Shoun Vanguard and the U. S. Tank Barge Hollywood 3013, Deer Park, Texas, October 7, 1986.* PB87-916408, NTSB/MAR-87/08.

National Transportation Safety Board. 1987. *Explosion and Fire Aboard the U.S. Tank Barge STC 410 at the Steuart Petroleum Company Facility, Piney Point, Maryland, December 20, 1986.* PB87-916409, NTSB/MAR-87/09.

National Transportation Safety Board. 1987. *Grouning of the Panamanian Tankship Grand Eagle in the Delaware River Near Marcus Hook, Pennsylvania, September 28, 1985.* PB87-916410, NTSB/MAR-87/10.

National Transportation Safety Board. 1988. *Ramming of the Maltese Bulk Carrier Mont Fort by the British Tankship Maersk Neptune in Upper New York Bay, February 15, 1988.* PB88-916409, NTSB/MAR-88/09.

National Transportation Safety Board. 1989. *Striking of a Submerged Object by the Bahamian Tankship Esso Puerto Rico, Mississippi River, Kenner, Louisiana, September 3, 1988.* PB89-916402, NTSB/MAR-89/02.

National Transportation Safety Board. 1989. *Explosion Aboard the Maltese Tank Vessel Fiona in Long Island Sound Near Northport, New York, August 31, 1988.* PB89-916403, NTSB/MAR-89/03.

National Transportation Safety Board. 1989. *Capsizing and Sinking of the Mobile Offshore Drilling Unit Rowan Gorilla I in the North Atlantic Ocean, December 15, 1988.* PB89-916406, NTSB/MAR-89/06.

National Transportation Safety Board. 1989. *Collision between the Swedish Auto Carrier Figaro and the French Tankship Camargue, Galveston Bay Enterance, November 10, 1988.* PB89-916407, NTSB/MAR-89/07.

National Transportation Research Board. 1989. *Exxon Valdez Casualty Factual Reports.*

National Transportation Safety Board. 1990. *Grounding of the U.S. Tankship Exxon Valdez on Bligh Reef Prince William Sound near Valdez, Alaska.* PB90-916405, NTSB/MAR-90/04.

National Transportation Safety Board. 1990. *Several Recent Ramming Investigated by the National Transporation Safety Board.* Presented to the Chesapeake Section of the Society of Naval Architects and Marine Engineers, June 5, 1990.

National Transportation Safety Board. 1991. *Grounding of the Greek Tankship World Prodigy Off the Coast of Rhode Island , June 23, 1989.* PB83-916401, NTSB/MAR-91/01.

UNITED STATES COAST GUARD

United States Coast Guard/National Transportation Safety Board. 1976. *SS C.V. Sea Witch - SS Sesso Brussels (Belgium); Collision and Fire in the New York Harbor on 2 June 1973 with Loss of Life.* Report no. USCG/NTSB MAR-75-6.

United States Coast Guard. 1977. *SS Sansinena (Liberian); Explosion and Fire in Los Angeles Harbor, California on 17 December 1976 with Loss of Life.* Report no. USCG 16732/71895.

United States Coast Guard. 1977. *M/V Elias; Explosion and Fire at Fort Mifflin, Pennsylvania on 9 April 1974 with Loss of Life.* Report no. USCG 16732/51363.

United States Coast Guard/National Transportation Safety Board. 1977. *SS Key Trader and SS Baune (Norwegian), Collision in the Mississippi River on 18 January 1974 with Loss of Life.* Report no. USCG/NTSB MAR-77-1.

United States Coast Guard/National Transportation Safety Board. 1977. *SS Edgar M. Queeny - S/T Corinthos; Collision at Marcus Hook, Pensylvania on 31 January 1975 with Loss of Life.* Report no. USCG/NTSB MAR-77-2.

United States Coast Guard. 1978. *Ocean Express (Drilling Unit); Capsizing and Sinking in the Gulf of Mexico on 15 April 1976 with Loss of Life.* Report no. USCG 16732/61865.

United States Coast Guard. 1978. *SS Frosta (Norwegian), M/V George Prince; Collision in the Mississippi River on 20 October 1976 with Loss of Life.* Report no. USCG 16732/73429.

United States Coast Guard. 1979. *M/V Chester A. Poling; Sinking in the Atlantic Ocean on 10 January 1977 with Loss of Life.* Report no. USCG 16732/73448.

United States Coast Guard. 1979. *Well Blowout with Explosion and Fire Onboard Penrod Drilling Rig 30 at South Marsh Island Block 281, Placid Oil Co. "C" Platform, on 5 March 1979, with Multiple Loss of Life and Pollution.* Report no. USCG16732-1/25/REF.

United States Coast Guard. 1982. *SS Ogden Willamette: Major Engine Room Flooding in the Caribbean Sea, Off of the Southeast Coast of Jamaica on 16 June 1982, with Personnel Injury.* Report no. USCG 16732/0210.

United States Coast Guard. 1983. *SS Marine Electric, O.N. 245675, Capsizing and Sinking in the Atlantic Ocean on 12 February 1983, with Multiple Loss of Life.* Report no. USCG 16732/0001 HQS 83.

United States Coast Guard. 1983. *SS Golden Dolphin: Explosion and Fire in the Atlantic Ocean on 6 March 1982 with Loss of Life.* Report no. USCG 16732/0002 HQS 82.

United States Coast Guard. 1985. *SS American Eagle, O.N. 278327, Explosion in the Gulf of Mexico on 26 February 1984 and Subsequent Sinking on 27 February 1984, with Loss of Life.* Report no. USCG 16732/0001 HQS 84.

United States Coast Guard. 1985. *Tankship Puerto Rican, O.N. 535000, Explosion and fire in the Pacific Ocean on 31 October 1984.* Report No. USCG 16732/0003 HQS 84.

United States Coast Guard. 1985. *Drillship Glomar Java Sea, O.N. 568182, Capsizing and Sinking in the South China Sea on 25 October 1983, with Loss of Life.* Report No. USCG 16732/0004 HQS 83.

United States Coast Guard. 1988. *SS Omi Yukon, D.N. 547919, Explosions and Fire on 28 October 1986 in the Pacific Ocean Approximately 1000 Miles West of Honolulu Hawaii with Multiple Loss of Life and Personnel Injuries.* Report no. USCG 16732/0002 HQS 88.

United States Coast Guard. 1990. *S/S American Trader (US)- Investigation Into the Grounding at Golden West Terminal Offshore Mooring on 7 February 1990 with Pollution and No Personnel Injuries.* Report no. USCG16732/MC90000938.

United States Coast Guard. 1992. *S/S Exxon Houston, Grounding Near Barbers Point, Hawaii on 2 MArch 1989, with Polution and Subsequent Constructive Loss to Vessel.* Report no. USCG16732/01 HQS 92.

MINERALS MANAGEMENT SERVICE

Minerals Management Service. 1984. *Investigation of July 20, 1983, Blowout Matagorda Island Block 657, Lease OCS-G-4139, Gulf of Mexico.* OCS Report MMS 84-0040.

Minerals Management Service. 1984. *Risk Analysis of Crane Accidents.* OCS Report MMS 84-0056.

Minerals Management Service. 1984. *Risk Analysis of Welding Accidents.* OCS Report MMS 84-0064.

Minerals Management Service. 1985. *Investigation of October 20-27 1983, Blowout, Eugene Island Block 10, Lease OCS-G 2892, Gulf of Mexico.* OCS Report MMS 85-0050.

Minerals Management Service. 1985. *Investigation of May 1984 Explosion and Fire, Lease OCS-G 3280, West Camaron Block 405, Gulf of Mexico Off the Louisiana Coast.* OCS Report MMS 85-0054.

Minerals Management Service. 1985. *Investigation of August 1984 Fire, Lease OCS-G 2254, East Camaron Block 322, Gulf of Mexico, Off the Louisiana Coast.* OCS Report MMS 85-0099.

Minerals Management Service. 1986. *Investigation of January 6, 1984, Flash Fire Ship Shoal Block 269, Gulf of Mexico, Off the Louisiana Coast.* OCS Report MMS 86-0101.

Minerals Management Service. 1986. *Investigation of December 1985 Blowout and Fire, Lease OCS-G 4268, West Cameron Block 648, Gulf of Mexico, Off the Louisiana Coast.* OCS Report MMS 86-0100.

Minerals Management Service. 1986. *Investigation of September 1984 Lowout and Fire, Lease OCS-G 5893, Green Canyon Block 69, Gulf of Mexico, Off the Louisiana Coast.* OCS Report MMS 86-0101.

Minerals Management Service. 1986. *Invesitgation of October 27-28, 1985, Structural Failures: Ocean Drilling and Exploration Company Platforms: Outer Continental Shelf Lease 0605, South Timbalier Block 86 and Outer Continental Shelf Lease 0073, South Pelto Block 19, Gulf of Mexico off the Louisiana Coast.* OCS Report MMS 86-0075.

Minerals Management Service. 1988. *Investigation of May 1987 Fire Lease OCS-G 2937 West Delta Block 109.* OCS Report MMS 88-0004.

Minerals Management Service. 1988. *Investigation of November 10, 1986 Blowout and Fire, OCS Lease 0244, West Cameron Block 71.* OCS Report MMS 88-0007.

Minerals Management Service. 1988. *Accidents Associated With Oil and Gas Operations: Outer Continental Shelf 1956-1986.* OCS Report MMS 88-0011.

Minerals Management Service. 1989. *Investigation of Fire September 1988 Lease OCS-G 1633, Main Pass Block 133.* OCS Report MMS 89-0072.

Minerals Management Service. 1989. *Investigation of Amoco Pipeline Company High Island Pipeline System Leak, Galveston Block A-2, February 7, 1988.* OCS Report MMS 89-0102.

Minerals Management Service. 1990. *Investigation of March 19, 1989, Fire South Pass Block 60 Platform B Lease OCS-G 1608.* OCS Report MMS 90-0016.

Minerals Management Service. 1990. *Accident Investigation Report OCS: Unocal P-0441.* Crane accident: November 25, 1990.

Minerals Management Service. 1991. *Accident Investigation Report OCS: Unocal P-0441.* Crane accident: January 7, 1991.

U.S. GEOLOGICAL SURVEY

Geological Survey. 1977. *An Investigation of Pennzoil's Blowout and Loss of Platform, High Island Block A-563, Gulf of Mexico Off the Texas Coast.* May, 1977.

Geological Survey. 1980. *Outer Continental Shelf Oil and Gas Blowouts.* Open File Report 80-101.

Geological Survey. 1980. *Investigation of March 198 Blowout and Fire, Lease OCS-G 2433, High Island Block A-368, Gulf of Mexico, Off the Texas Coast.* Open File Report 80-1278.

Geological Survey. 1981. *Investigation of August 1980 Blowout and Fire, Lease OCS-G 4065, Matagorda Island Block 669, Gulf of Mexico Off the Texas Coast.* Open File Report 81-706.

Geological Survey. 1981. *Investigation of January 1981 Blowout and Fire, Lease OCS-G 4077, High Island Block 38, East Addition, Gulf of Mexico Off the Texas Coast.* Open File Report 81-868.

Geological Survey. 1981. *Investigation of August 1980 Blowout and Fire, Lease OCS-G 2271, Vermilion Block 348, Gulf of Mexico Off the Louisana Coast.* August, 1991.

Geological Survey. 1983. *Investigation of October 1982 Blowout and Fire, Eugene Island Block 361, Gulf of Mexico.* Open File Report 83-113.

Geological Survey. 1983. *Outer Continental Shelf Blowouts: 1979-1982.* Open File Report 83-562.

ADDITIONAL ACCIDENT REPORT AND ACCIDENT DATA SOURCES

California State Lands Commission. 1991. *Chevron El Segundo Oil Spill Report.* Marine Facilities Inspection and Management Division.

CASMAIN, USCG casualty database. 1981-1990.

McLeod, J. 1992. *The Oil Spill...Arco...the Pilot's Story.* (The grounding of the *Arco Anchorage*. Port Angeles, WA, 1985).

Moan, T. 1981. *The Alexander Kielland accident.* Report of the Norwegian Government Commission. April 21, 1981.

Report of the Royal Commission on the *Ocean Ranger* Marine Disaster. 1985. Ottawa, Ontario, Canada.

Reading and Bates Offshore Drilling Company. 1971. *Loss of the C.E. Thorton,* February 13, 1971.

United Kingdom Department of Energy. 1988. *Piper Alpha Technical Investigation: Interim Report.* (Petrie Report) Crown: London. September, 1988.

United Kingdom Department of Energy. 1988. *Piper Alpha Technical Investigation: Further Report.* (Petrie Report) Crown: London. December, 1988.

United Kingdom Department of Energy. 1990. *The Public Inquiry into the Piper Alpha Disaster*, The Hon Lord Cullen, Volume 1, HMSO Publications, London. November, 1990.

United Kingdom Department of Energy. 1990. *The Public Inquiry into the Piper Alpha Disaster*, The Hon Lord Cullen, Volume 2, HMSO Publications, London. November, 1990.

Veritec. 1984. *Offshore Reliability Data Handbook* (OREDA), 1st Edition. Penn Well Books.

Veritec. 1989. *The Worldwide Offshore Accident Databank* (WOAD). Annual Reports through 1988. Oslo, Norway.

APPENDIX 3

HESIM, HOEDQS, and Influence Diagram User Instructions

HOEDQS - HESIM

This first version of the HOEDQS-HESIM has been designed to run in an Apple Macintosh II, Centris 600, or Powerbook 160 or better domain using Microsoft Excel version 4.0 software package. A color monitor is preferred but not necessary. Best results are seen when using a math co-processor and at least 5K of random access memory (RAM). Future versions of the HOEDQS-HESIM will be designed for use in both PC-DOS and Macintosh environments. For the descriptive background of the HOEDQS and the HESIM, please refer to Chapter 5.

To Start

1. Open "HOEDQS" Disk by double clicking on the HOEDQS Icon or name.
2. Open the Microsoft Excel document entitled "HOEDQS".
3. The startup window appears; click on the "OK" button to engage the HOEDQS.
4. A window will appear asking if you wish to input/analyze data or perform a HESIM analysis. Click on the appropriate option button and then click on the "OK" button or press Return.

Inputting or Analyzing Data

5. A window will appear asking if you wish to input data or analyze data. Click on the appropriate option button and then click on the "OK" button or press Return.

Inputting Data:

6. A window appears asking if the user wishes to input new or modified data. Click on the appropriate option button and then click the "OK" button. If the data is new, it will open a new set of data inputs in the database. If it is a modified assessment, it searches for the selected vessel or platform, and recall that information.
7. A window entitled "Vessel/Platform Identification" will appear. Input all of the appropriate information relevant to the vessel or platform near miss or casualty.

This input information cannot include the following symbols: "", /, - , +, =. A "bottom line" (_) is suggested to separate words or phrases.

8. If the input data is new data, a window entitled "Casualty Values" will appear. The user inputs the appropriate information. Leave all non-applicable boxes blank. If you are inputting data for a near miss, input zeros in each box. Click on the "OK" button or press Return.

9. A window entitled "Casualty Level" will appear asking what casualty level the user wishes to input information for. Click on the appropriate option button then click on the "OK" button.

10. If the user selects the "Underlying" button for the casualty level, a window will appear entitled "Underlying EDAs". Under the "Primary" heading, there is a drop-down box with 17 events, decisions, or actions that can be selected as the primary underlying contributor to the casualty or near miss. If none of the primary factors do not relate to the primary underlying EDA, select the last input in the primary drop down box entitled "other (type in box below)". Type the underlying contributing factor in the edit box.

    If the user selects the "Direct" or "Compounding" button for the casualty level, a window will appear entitled either "Direct EDAs" or "Primary EDAs". Under the "Primary" heading, there is a drop-down box with 17 events, decisions, or actions that can be selected as the primary underlying contributor to the casualty or near miss. No special input edit box will appear for the "Direct EDAs" or "Compounding EDAs" windows.

    The user has the option of selecting 6 associated EDAs for inputting human error data. There are 39 associated EDAs from which a selection can be made.[1] These associated EDAs influence or are directly related to the primary EDA and are input as appropriate. Once all associated EDAs are selected, press the "OK" button or press Return.

11. A window will appear asking the user which EDA for the particular casualty level (Underlying, Direct, or Compounding) they wish to input data for. Select the EDA by clicking on the appropriate option button then press the "OK" button or press Return. A spreadsheet window entitled "HOEDQS spreadsheet" should appear with the user interface window shown in Figure A3.1.

The HOEDQS spreadsheet

12. The "HOEDQS spreadsheet" window has been designed to be a user friendly window for users to input or analyze data. The set of yellow cells in the upper left hand corner of the HOEDQS spreadsheet are used to provide the casualty identification, level and other related factors. The casualty-near miss information input by the user in the "Vessel/Platform Information" window is provided in the first three rows and two columns. The Casualty Level, and Casualty Factor (EDA) are provided below the vessel/platform information. Inputs for system and task complexities are provided in the next set of rows and columns. The task and system inputs are left blank until the values are input by first selecting the "Task Complexity" and "System Complexity" buttons (see Table A3.1).

---

[1] These associated EDA's are selected from the U.S. Coast Guard's Marine Casualty Human Factor Supplement (MCHFS). Each of these factors are defined at the end of Appendix 3.

Figure A3.1 - HOEDQS spreadsheet user interface window

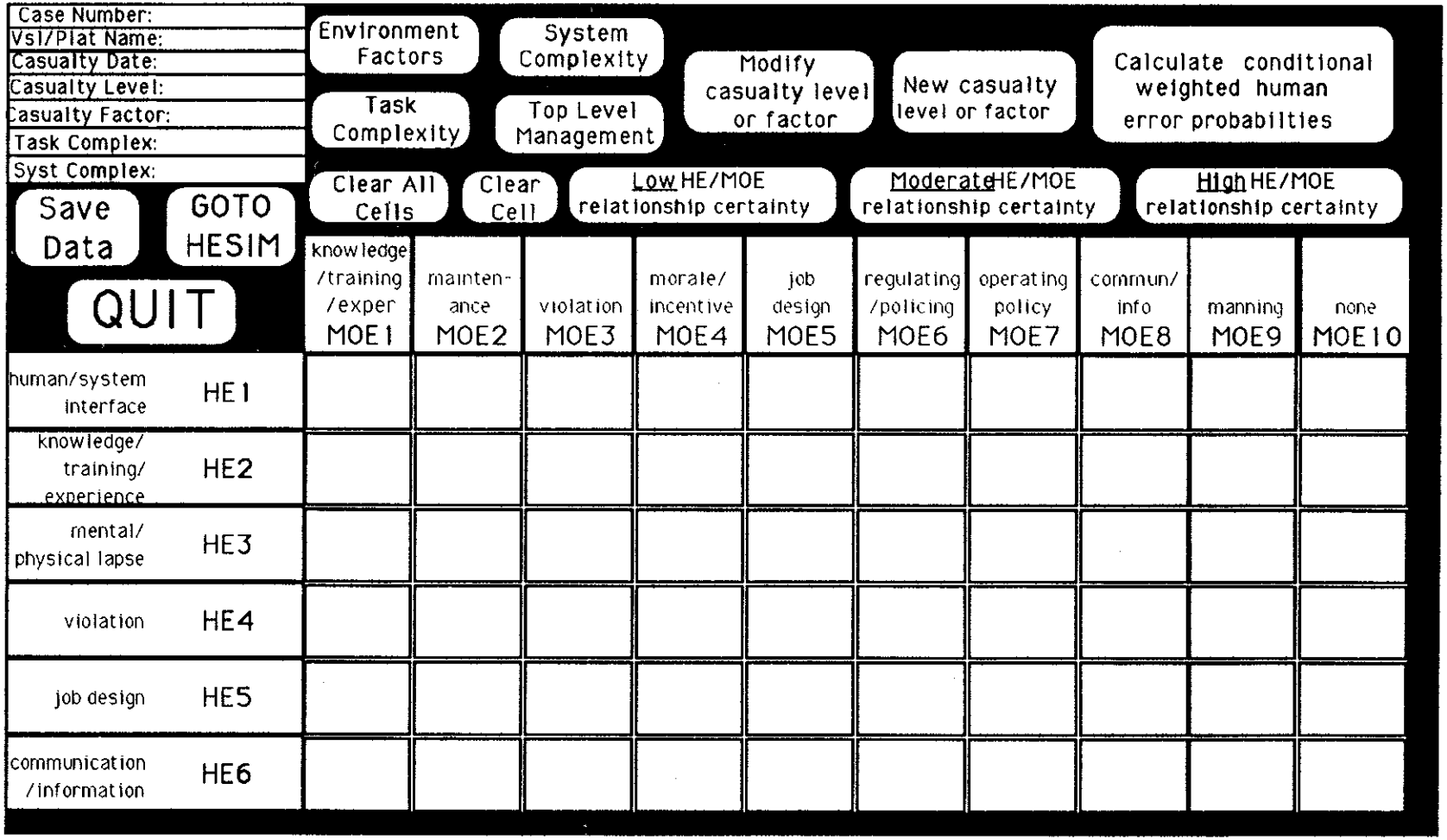


Table A3.1: Button description for HOEDQS spreadsheet

Button	Description
Save Data	Saves the data to the database
GOTO HESIM	Activates the "HESIM worksheet" window to perform HESIM analysis.
QUIT	Quits the HOEDQS program.
Environmental Factors	Activates the window entitled "Environmental Factors" for the user to input environmental inhibitors that are contributors to the EDA being analyzed. The questions and answers are provided below in *Environmental Factors*.
Task Complexity	Activates the window entitled "Task Complexity" for the user to input whether the task complexities are "High" or "Low" for the EDA being analyzed (if applicable).
System Complexity	Activates the window entitled "System Complexity" for the user to input whether the system complexities are "High" or "Low" for the EDA being analyzed (if applicable).
Top Level Management	Activates the window "Top Level Management" for the user to input top-level management factors described in Section 4.4.3. The questions and answers are provided below in *Top Level Management Questions*.
Modify casualty level or factor	This will return the user to the "Casualty Level" window so the user may select the casualty level that they wish to modify data for. The user is then provided with the window to select the casualty EDA to be performed. Once the relevant information is provided, the HOEDQS will find the record in the database and return the information to the "HOEDQS spreadsheet" for modification.
New casualty level or factor	This will return the user to the "Casualty Level" window so the user may select the casualty level that they wish to modify data for. The user is then provided with the window to select the casualty EDA to be performed.
Clear All Cells	Clears all human and organizational error inputs for the particular accident EDA.
Clear Cell	Once this button is clicked, the user has the option of clearing any human and organizational error input cell they so choose by double-clicking on the cell.

Table A3.1: Button description for HOEDQS spreadsheet (cont.)

Button	Description
Low HE/MOE relationship certainty	Once this button is clicked, the user has the option of inputting into any human and organizational error input cell a "Low" HE/MOE certainty level for the human and organizational error of interest. This is performed by double-clicking on the cell. This will return the letter "L" in the cell.
Moderate HE/MOE relationship certainty	Once this button is clicked, the user has the option of inputting into any human and organizational error input cell a "Moderate" HE/MOE certainty level for the human and organizational error of interest. This is performed by double-clicking on the cell. This will return the letter "M" in the cell.
High HE/MOE relationship certainty	Once this button is clicked, the user has the option of inputting into any human and organizational error input cell a "High" HE/MOE certainty level for the human and organizational error of interest. This is performed by double-clicking on the cell. This will return the letter "H" in the cell.
Calculate conditional weighted human error probabilities	Calculates the weighted human error probabilities as described below in *Analyzing Accident Data*. The weighted probability of that criteria is then calculated as described in Section 4.5.2.

13. The user now has the opportunity to input the related human, organizational, environmental, task, and system information relevant to the EDA. Each of the human and organizational errors are arranged in a matrix form as shown in Figure A3.1.

    The user has the option of inputting the error certainties into the cells directly, by typing them in from the keyboard, or using the certainty level buttons described in Table A3.1. If the user inputs the certainty levels in manually, they should be in uppercase letters: "L" (low), "M" (moderate), and "H" (high).

    There are 15 buttons on the HOEDQS spreadsheet that utilize a number of functions for inputting casualty or near-miss information. Table A3.1 provides a short description of each button on the HOEDQS spreadsheet.

Using HOEDQS spreadsheet buttons

Environmental Factors:

14. After clicking on the "Environmental Factors" button, a window will appear asking the user to input all relevant external and internal environmental factors. More than one environmental factor may be selected. Using the mouse the user clicks on the appropriate organizational factors and an "X" will appear in the box. Once the user has selected all environmental factors, click the "OK" button or press Return.

Task Complexity:

15. After clicking on the "Task Complexity" button, a window will appear asking the user to select whether the task complexity for the EDA was high or low. The user

selects the appropriate button then selects the "OK" button or press Return. The task complexity level will appear as either "LOW" or "HIGH" in the yellow "Task Complex" cell in the upper left hand corner of the HOEDQS spreadsheet.

System Complexity:

16. After clicking on the "System Complexity" button, a window will appear asking the user to select whether the system complexity for the EDA was high or low. The user selects the appropriate button then selects the "OK" button or press Return. The system complexity level will appear as either "LOW" or "HIGH" in the yellow "Syst Complex" cell in the upper left hand corner of the HOEDQS spreadsheet.

Top-Level Management:

17. It is not required that this information be provided for all EDAs but should be included where relevant. If the information is relevant, after clicking on the "Top Level Management" button, a window entitled "Top-Level Management (TLM) Part 1" will appear. This window includes 3 of 5 questions related to the impact of top-level management (TLM) upon the EDA (see Table A3.2). Select the appropriate information that best suits the organization in question then select the "OK" button or press Return. A second window will appear entitled "Top-Level Management (TLM) Part 2" that provide the last 2 questions of Table A3.2. Select the appropriate information that best suits the organization in question then select the "OK" button or press Return. The user is then returned to the "HOEDQS spreadsheet" window.

Modify Casualty Levels or Factors:

18. By selecting the "Modify casualty level or factor button", the "Casualty Level" window will appear so the user may select the casualty level for which they wish to modify data. The user is then provided with the window to select the casualty EDA to be performed. Once the user selects the casualty EDA, the HOEDQS will find the record in the database and return the information to the "HOEDQS spreadsheet" for modification. (Note: The user will notice that all relevant information has changed in the casualty-near miss information provided in the yellow cells in the upper left hand corner of the "HOEDQS spreadsheet").

New Casualty Levels or Factors:

19. By selecting the "New casualty level or factor button", the "Casualty Level" window will appear so the user may select the casualty level for which they wish to input new data. The user is then provided with the appropriate window to select a new set of EDAs as described above in (10) and (11). Once the EDA is selected, the HOEDQS returns the user to the "HOEDQS spreadsheet" for input. (Note: The user will notice that all relevant information has changed in the casualty-near miss information provided in the yellow cells in the upper left hand corner of the "HOEDQS spreadsheet").

Saving Data into the Spreadsheet:

20. Once the user has input all of the information for the specific EDA, press the "Save Data" button. If the data is new, it will be written into the database as a new record, if modified data it overwrite the previous information in the database.

Analyzing Accident Data:

21. There are two options for analyzing accident data. First, the user has the option of selecting to initially analyze accident data by selecting the "Analyze data" button when viewing the window described in (5) above. The other option is by directly selecting the "Calculate conditional weighted human error probabilities" button on the HOEDQS spreadsheet.

Table A3.2: Top Level Management Questions in the HOEDQS

1. How would you rate TLM's overall commitment to safety? a. *Excellent* b. *Good* c. *Moderate* d. *Poor*
2. What is TLM's commitment to long term safety goals at the front-line operator level? a. *Proactive*: Regular review and updating of SMS by TLM. Actively searching for better HOE management alternatives. b. *Calculate*: Concerned with engineering "techno-fixes" as means of addressing human errors. Management uses various safety auditing techniques to identify and assess human operator errors. c. *Reactive*: Stays at or just above minimum safety standards. Little or no foresight in addressing human errors at the operator level.
3. Are those at the TLM level cognizant of the problems that occur at the front-line operator levels with regard to operational safety? In other words, is there a direct feedback between TLM and front line operators? a. *Always* b. *Most times* c. *Sometimes* d. *Never*
4. Does TLM assign competent personnel (consultants, mid-level management, front-line operators, etc.) to address problems that occur at the front-line level? a. *Always* b. *Most times* c. *Sometimes* d. *Never*
5. Does TLM assign sufficient resources (capital, time, expertise) to addressing safety goals and management at the front-line operator level? a. *Always* b. *Most times* c. *Sometimes* d. *Never*

A window will appear entitled "Accident Frequency Search". The user has the option of selecting the data criteria for which to calculate a weighted probability. The window has 7 drop down boxes for human errors, organizational errors, casualty level, EDA, task complexity, system complexity, and error certainty level. At the bottom of the window, the user has the option to either include all environmental factors or just the environmental factors that are selected. Once the relevant criteria has been selected, click on the "OK" button or press Return.

A window will appear asking the user to input the number of operations per unit time. Input the appropriate number into the appropriate box then press the "OK" button or Return.

Four weighted probabilities are then calculated and presented in a window that appears after the calculations are performed. These probabilities are:

(a) Probability of human error, organizational error, casualty level, EDA, task complexity, system complexity, and certainty level criteria selected in the "Accident Frequency Search" window.

(b) Probability of human error conditional upon organizational error, casualty level, EDA, task complexity, system complexity, and certainty level criteria selected in the "Accident Frequency Search" window.

(c) Probability of human error, casualty level, EDA, task complexity, system complexity, and certainty level criteria selected in the "Accident Frequency Search" window, and all organizational errors.

(d) Probability of human error conditional upon casualty level, EDA, task complexity, system complexity, and certainty level criteria selected in the "Accident Frequency Search" window, and all organizational errors.

To the left of the window all of the relevant "Error Solicitors" criteria that the HOEDQS searched for in the database are listed. Once this data is recorded by the user, press the "OK" button or Return. This will return the user to the "HOEDQS spreadsheet" window.

Quitting:

22. To quit the HOEDQS program, press the "QUIT" button. If the user wishes to save the data in the HOEDQS spreadsheet, the "Save Data" button should be pressed before pressing the "QUIT" button. This will save all information to the information currently in the HOEDQS spreadsheet to the database. Once the user quits the HOEDQS spreadsheet is cleared of all information.

The Human Error Safety Index Method

To Start the HESIM

23. The Human Error Safety Index Method (HESIM) session can be started in two ways. The first way is by selecting the appropriate option button at Step 4 above (see (4)). The second way to start a HESIM session is to select the "GOTO HESIM" button on the HOEDQS spreadsheet.

24. The startup window appears; click on the "OK" button to engage the HESIM.

25. The window appears stating that you are ready to start your HESIM session click on the "OK" button to begin.

26. The "Accident Frequency Search" window will appear. The user has the option of selecting the data criteria for which to calculate a weighted probability. The window has 7 drop down boxes for human errors, organizational errors, casualty level, EDA, task complexity, system complexity, and error certainty level. At the bottom of the window, the user has the option to either include all environmental factors or just the environmental factors that are selected at the left. Once the relevant criteria has been selected, click on the "OK" button or press Return.

    A window appears asking the user to input the number of operations per unit time. Input the appropriate number into the appropriate box then press the "OK" button or Return.

27. A window appears describing the HESIM worksheet format. After reading the information in the window, press "BEGIN" or Return.

28. A window entitled "HESIM worksheet" appears. The HESIM worksheet format provides the user with two numbers in the human and organizational error matrix. The upper value (in red) is the *overall human error safety index* ($SI_{HEi,OEj,HF,Syst,Environ,EDA}$). The lower value (in black) is the *human error safety index* ($SI_{HEi|OEj,HF,Syst,Environ,EDA}$).

29. As shown in Figure A3.2 are 10 buttons on the HESIM worksheet that utilize a number of functions for providing quantitative measurements for human errors conditional upon various operating conditions. Table A3.3 provides a short description of each button on the HESIM worksheet.

Using HESIM worksheet buttons

Goto Data Inputs:

30. After clicking on the "GOTO DATA INPUTS" button, the same window appears as in Step 5 (see (5) above) asking the user whether he/she wish to input or analyze data. The user then follows Steps 6-22 described above related to the data input and analysis.

Organizational Safety Index:

31. After clicking on the "Organizational Safety Index" button, a window appears entitled "MOE Weights for EDA: EDA". For the particular EDA, the user has a listing of the 9 MOEs described in Chapter 5. The user selects the MOE for which they wish to assign TLM factors by clicking on the appropriate option button. The user then proceeds to input the percentage values by which (in their best judgment and experience) they feel the impact of the TLM factor has upon preventing or mitigating those types of errors for that particular EDA. Recall that the TLM factors are those described and presented in Chapter 5. The default values for each of the TLM factors is 20%.

Table A3.3: Button description for HESIM worksheet

Button	Description
GOTO DATA INPUTS	Activates the "HESIM worksheet" window to perform HESIM analysis.
QUIT	Quits the HOEDQS program.
Organizational Safety Index	Activates windows to assess impacts of organizational factors on the overall safety index.
Human Factor Safety Index	Activates windows to assess impacts of stress and routineness factors on the overall safety index.
Task Safety Index	Activates windows to assess impacts of task complexities on the overall safety index.
System Safety Index	Activates windows to assess impacts of system complexities on the overall safety index.
Environmental Safety Index	Activates windows to assess impacts of external and internal environmental factors on the overall safety index.
UPDATE SAFETY INDICES	Updates the human error safety index. (Note: Does not update the overall human error safety index.)
SELECT NEW DATA CRITERIA	Activates the "Accident Frequency Search" window to select new data criteria for the HESIM.
Calculate Marginal HE/OE Indices	This button calculates the marginal human error safety indices by taking a weighted average of each human error for all organizational errors.

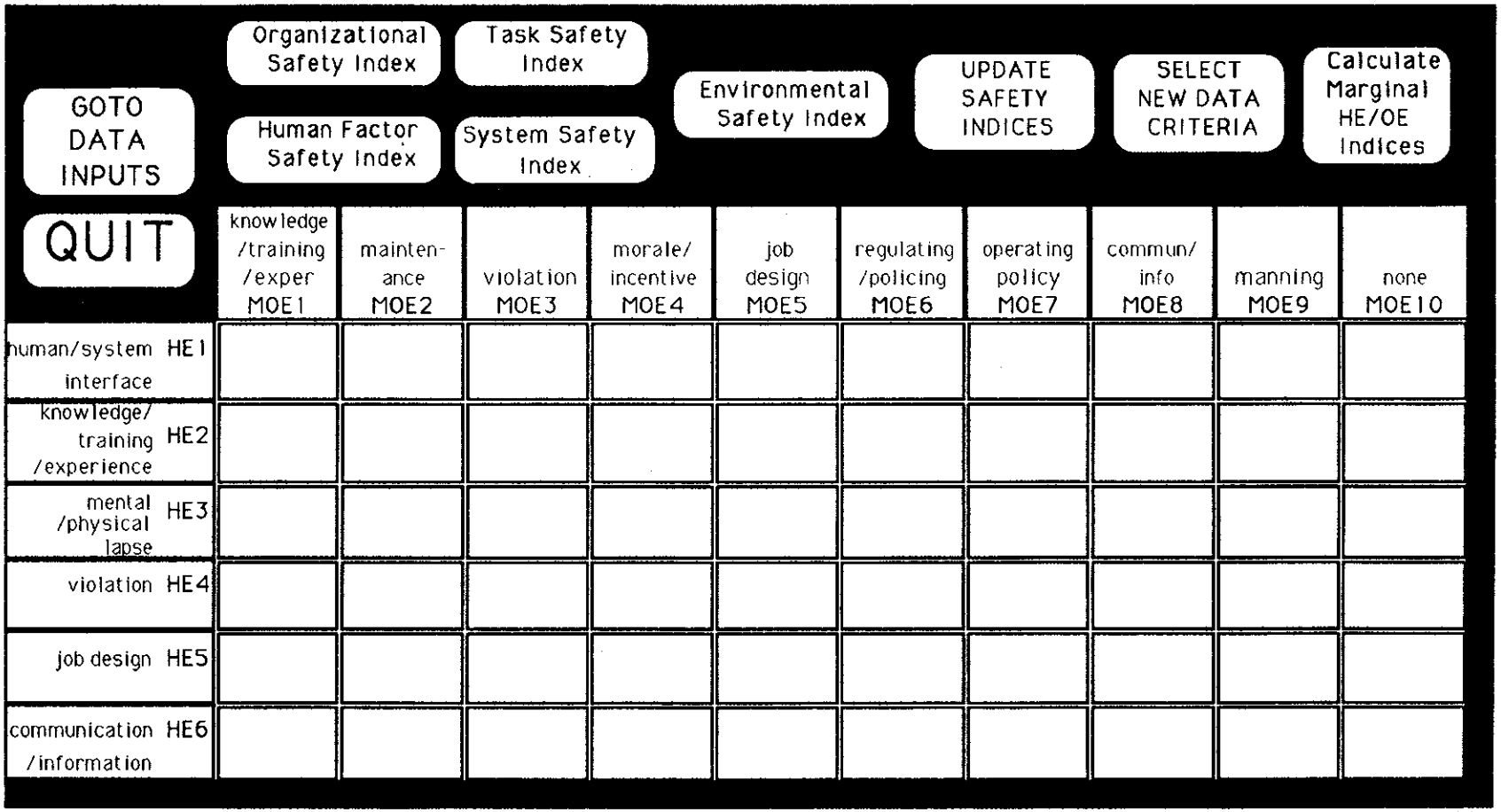
At the bottom of the window, the user inputs the minimum default value that, in their best judgment, relates to the impact of TLM factors upon MOE errors for the EDA in question. As shown in Equation 5.9, the maximum value between the weighted calculations and the minimum default value is used for the organizational error index. The user then clicks on the "OK" button or presses Return.

32. If the user inputs the values such that they do not add up to 100%, a window appears stating that the overall weights inputted are not equal to 100%. It then returns the user to the "MOE Weights for EDA: EDA" window for correction.

33. A window then appears entitled "MOE SI for EDA: EDA". The user then inputs the maximum degree (in their judgment) by which the specified MOE affect the risk of the system. The maximum degree value is described by stating the degree by which the risk is increased by that MOE for the EDA in question for the worst possible case. The default value is 1. Example: If the risk is doubled for human system interface errors for a grounding event, the user would input a value of "2" in the edit box. The user then clicks the "OK" button or presses Return.

34. A window then appears entitled "TLM/MOE Relation for EDA: EDA". For the MOE and EDA in question, the user then inputs whether they feel that TLM is either "sufficient" or "insufficient" in addressing the 5 TLM factors. The user selects the appropriate option button for each TLM factor and then clicks the "OK" button or presses Return.

Figure A3.2 - HESIM worksheet user interface window



35. A window appears entitled "TLM Weights for EDA: EDA" asking whether the user wishes to return to the input additional organizational error index information or return to the HESIM worksheet window. If the user returns to input additional data, follow Steps 31 through 34. If the user wishes to return to the HESIM, move on to Step 36.

36. A window appears asking the user to input (in their best judgment) the ratings of each MOE in affecting the prevention or mitigation of human errors at the operator level for the EDA of interest. Once the user inputs these ratings click on the "OK" button or presses Return. This will return the user to the "HESIM worksheet" window.

Human Factors Index:

37. After clicking on the "Human Factors Safety Index" button, a window appears asking the user to input the maximum degree (in their judgment) by which the stress and routineness affect the risk of human errors for the EDA. The maximum degree value is described by stating to what degree the risk is increased by stress and routineness for the EDA in question in the worst possible case. The default values are 1 for both stress and routineness. Once the values are input into the edit boxes, the user then clicks the "OK" button or presses Return.

38. A window appears asking the user to rate the effects of the human factors on the EDA in question. The EDA is shown at the top of the window. These can be "High", "Moderate ", or "Low " stress and complexity. The user selects option buttons that best describe stress and routineness for that EDA. The user then clicks the "OK" button or presses Return.

Task Safety Index:

39. After clicking on the "Task Safety Index" button, a window appears asking the user to inputs the maximum degree (in their judgment) by which the stress and routineness affect the risk of human errors for the EDA. The maximum degree value is described by stating to what degree is the risk increased by task complexity for the EDA in question in the worst possible case. The default values are 1 for both stress and routineness. Once the values are input into the edit boxes, the user then clicks the "OK" button or presses Return.

40. A window appears asking the user to rate the effects of task complexities on the EDA in question. The EDA is shown at the top of the window. These can be "High complexity", "Moderate complexity", or "Low complexity". The user selects the option buttons that best describe stress and routineness for that EDA. The user then clicks the "OK" button or presses Return.

Environmental Safety Index:

41. After clicking on the "Environmental Safety Index" button, a window appears asking the user to inputs the maximum degree (in their judgment) by which the external and internal environmental factors affect the risk of human errors for the EDA. The maximum degree value is described by stating to what degree is the risk increased by both external and internal environmental factors for the EDA in question in the worst possible case. The default values are 1 for both stress and

routineness. Once the values are input into the edit boxes, the user then clicks the "OK" button or presses Return.

42. A window appears asking the user to rate the effects of both external and internal environmental factors (inhibitors) on the EDA in question. The EDA is shown at the top of the window. These can be "High", "Moderate", or "Low". The user selects the option buttons that best describe stress and routineness for that EDA. The user then clicks the "OK" button or presses Return.

UPDATE SAFETY INDICES:

43. After clicking on the "UPDATE SAFETY INDICES" button, each human error safety index is updated to account for any modifications that are made in the organizational, human factor, task, or system indices described above. This does not update the overall human error safety index.

SELECT NEW DATA CRITERIA:

44. The function of the "SELECT NEW DATA CRITERIA" button is to perform HESIM analysis for human errors for any of the established human, organizational, system, task, environmental, or certainty level criteria.

    After clicking on the button "SELECT NEW DATA CRITERIA", the "Accident Frequency Search" window will appear. The window has 7 drop down boxes for human errors, organizational errors, casualty level, EDA, task complexity, system complexity, and error certainty level. There are also selection boxes to include specific (or all) organizational factors. At the bottom of the window, the user has the option to either include all environmental factors or just the environmental factors that are selected at the left. Once the relevant criteria has been selected, click on the "OK" button or press Return.

45. The next window that appears asks the user to input the number of operations per unit time of interest. Input the value into the edit box the click on the "OK" button or press Return.

46. A window appears describing the HESIM worksheet format. After reading the information in the window, press "BEGIN" or Return. This returns the user to Step 28 described above.

Calculate Marginal HE/OE Indices:

47. After clicking the "Calculate Marginal HE/OE Indices" button, the "Risk Index = 1-Safety Index" window will appear. This window displays the marginal risk indices for each human error conditional upon the Error Index Criteria. The Error Index Criteria are presented on the right hand side of the window. By clicking on the "OK" button or pressing Return, the user is returned to the "HESIM worksheet" window.

Quitting:

48. To quit the HOEDQS and HESIM program, press the "QUIT" button. Once the user quits the HESIM worksheet, all information is cleared.

INFLUENCE DIAGRAMS: 4 Case Study Examples

This first version of the influence diagram models described in Chapter 7 have been designed to run in a PC-DOS environment using *InDia™* version 2.0 by Decision Focus Incorporated. For a background of the basics for using and operating *InDia™* please refer to the *Professional Edition of InDia™: Users Guide* [Decision Focus Incorporated, 1991]. Best results are seen when using a math co-processor and at least 5K of random access memory (RAM). For the descriptive background of the model templates, please refer to Chapter 7.

To Start

1. Once the user has begun the *InDia™* program, click on "Diagram" in the toolbar at the top of the window.

2. A drop-down box will appear. Click on "Load" in the drop-down box.

3. Another drop-down box will appear. Click on "Load Any Diagram" in the drop-down box.

4. A window will appear entitled "Load Diagram". To select the influence diagram they wish to load, double-click on the name of the influence diagram. The user can also select any influence diagram they wish by directly specifying the path of where to find the diagram. The user then clicks on the "Ok" button. Table A3.4 is a listing of the four templates described in Chapter 7.

Table A3.4: Influence diagram templates

Operational Model	Model identification in *InDia™*[2]
Tanker grounding-collision	"EV1*.ID"
Tanker grounding-collision: tug support alternative	"EV2*.ID"
Platform production-maintenance: simultaneous maintenance and production	"PALPHA2*.ID"
Platform production-maintenance: gas leak detection and control	"PALPHA3*.ID"
Vessel load-discharge	"LDDSCHG*.ID"
Offshore crane operations	"CRANE*.ID"

5. The selected diagram will appear in a new window.

6. Please refer to the *Professional Edition of InDia™: Users Guide* for information on analyzing the diagrams.

---

[2] The "*" represents that there are a number of values that are represented in that position.

APPENDIX 4

Human And Organizational Error Model Development And Analysis Framework Guide

The development and analysis framework is a consolidation of the modeling processes described in Chapters 3-6. The guide is used as a quick reference to assist the user in the qualitative and quantitative modeling process. Figure A4.1 is a guidance map for the HOE process including the chapter where each topic is found within the text. The framework guide is an overview of the primary topics of the modeling procedure: (1) framework modeling (post-mortem and existing operations), (2) probability encoding, (3) HOE data collection, and (4) sensitivity analysis. The *Human Factor Safety Index Method* is described in Chapter 5.

HOE FRAMEWORK DEVELOPMENT

Post-mortem Study

1. Identify relevant events, decisions, and actions for the accident classes of particular interest. The class of accidents should be well defined and well documented to allow for accurate modeling of as many contributing factors as possible.

2. Construct an influence diagram representation modeling the influences between contributing casualty solicitors (events, decisions, actions). The representation is an integration of available accident data and heuristic judgment of the experts constructing the model. Use the accident data and heuristic judgments to relate contributing HOE's to the events, decisions, and actions occurring in the accident sequence.

3. Eliminate casualty factors from the influence diagram representation which particularly unique to the accident scenario. The goal is to produce a template diagram which preserve the central causative mechanisms of the particular casualty while eliminating unique accident contributors. Casualty factor variables can be eliminated by heuristic judgments and sensitivity analysis (see below).

4. Determine whether the template model state variables are deterministic or probabilistic through sensitivity analysis. Perform sensitivity analysis upon decision variables to determine whether they should be removed from the model.

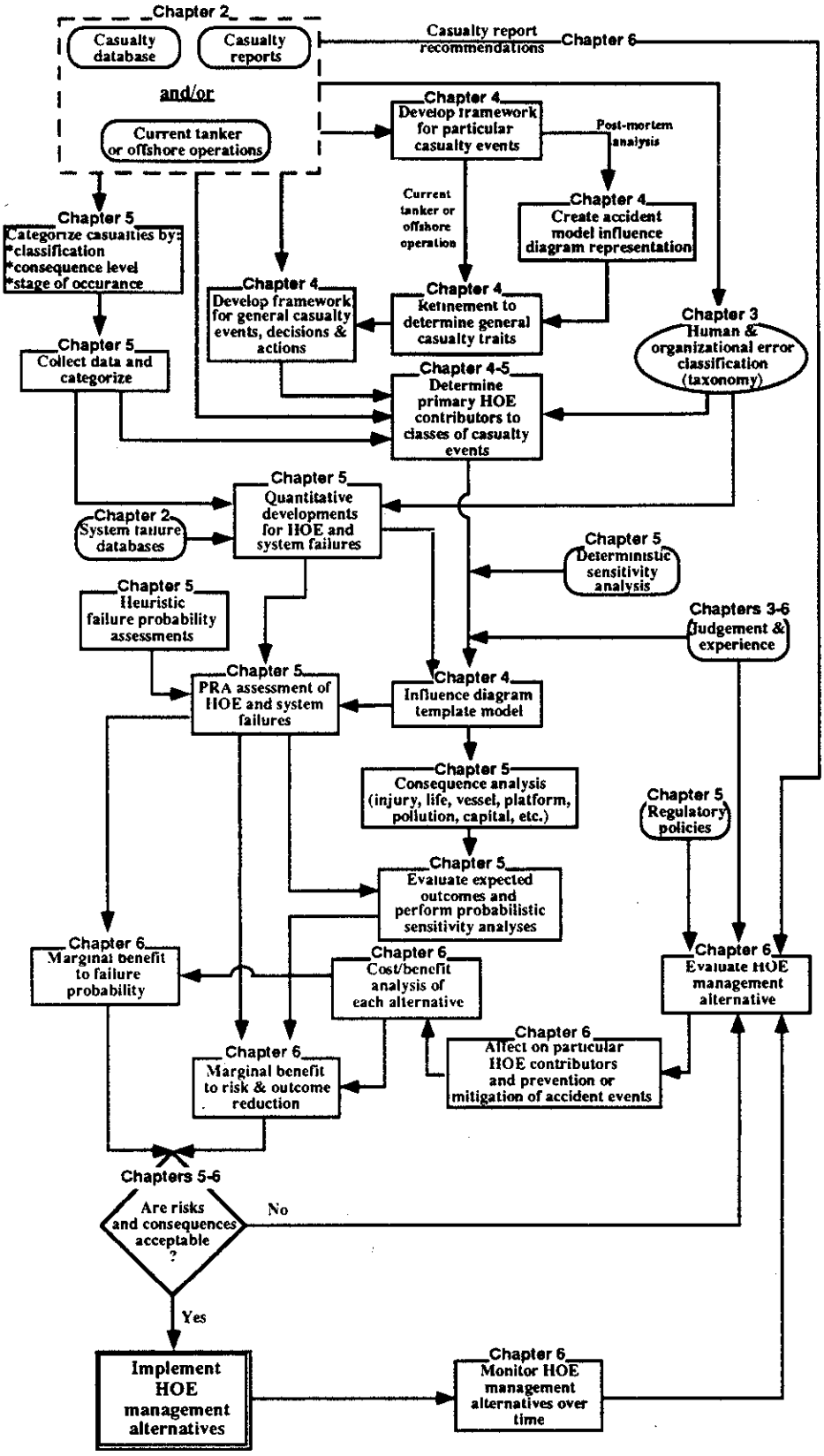


Figure A4.1 - HOE flowchart for project

Existing Operations

1. Identify relevant events, decisions, and actions leading to determining accident scenarios. Use available near miss and casualty data, experiences, and judgments. The class of accidents should be well defined to allow for accurate modeling of as many contributing factors as possible.

2. Use expert opinion, reports, and data to construct a template diagram identifying primary accident contributors (events, decisions, actions, scenarios) to the particular class of accidents being modeled. The goal is to produce a template diagram which preserve the central causative mechanisms of the particular casualty while eliminating unique accident contributors. Casualty factor variables can be eliminated by heuristic judgments and sensitivity analysis (see below).

3. Determine whether the template model state variables are deterministic or probabilistic through sensitivity analysis. Perform sensitivity analysis upon decision variables to determine their importance upon in the model.

QUANTITATIVE ASSESSMENT

Probability Encoding

There are five general steps to the encoding process as described by Spetzler and Staël von Holstein (1972) and are described in the following sections.

1. *Motivating*:
   Developing a rapport with the experts involved in the modeling and decision process to identify any possible motivational biases. The goals of this phase are to introduce the experts to the encoding tasks and difference between deterministic and probabilistic predictions of variables. In addition, this step allows the interviewer an opportunity to explore for motivational biases of the experts (subjects).

2. *Structuring*:
   This step is important to identify uncertain quantities to be defined in the model. This step entails clearly communicating the model variables. The experts should be able to pass what is called the *clairvoyance test*: a clairvoyant should be able to specify the outcome of variables without asking additional questions. For example, if "vessel traffic" is a variable, it does not specify the location, time of day, etc. However, the variable was identified as vessel traffic in the Valdez Narrows of Prince William Sound, then the information is much clearer in its interpretation.

3. *Conditioning*:
   Conditioning is necessary in the development of fundamental judgments and avoidance of cognitive biases. The primary goals is to communicate with the expert group to ensure all members are using the same group of assumptions and are perceiving the problem in the same structured way.

   This step is the important in identifying bias. Here the experts are asked to identify the sources of the values they have assigned to each of the variables. For example, if an expert identifies a realistic high consequence (e.g. 10 people injured) for a particular accident event, the interviewer would ask from what source is the judgment being derived? Does it parallel a recent similar accidents?

4. *Encoding*:
The encoding step is the direct quantification of heuristic judgments in terms of probability assignments. Distinction are made between direct human related factors (HOE's, decisions and actions) and events or consequences. Human related factors are dependent upon the error classifications described in Chapter 3.

Probabilistic encoding of events and consequences are assessed to arrive at cumulative distributions for magnitudes of accident events. We may estimate events and consequences by the following method:

(a) Ask for extreme value event (low and high) assignments of casualty consequences. This provides a set of boundaries in which the probability modeling will occur (see Chapter 5). Generally, the larger the spread, the greater the uncertainty.

(b) Ask for the probability or odds of the extreme values. Elicit some scenarios that may assist in the value assignments.

(c) Explore values between the extreme values by using the *interval technique*. The interval technique entails splitting an interval into two sections and asking which part the expert agrees is most likely. The dividing point is changed until the subject is indifferent between the intervals. This point is recorded as the median value. The intervals are further sub-divided and the process repeated. The quartile values are obtained and recorded. The intervals may be further subdivided and the method repeated but may be subjected to compounding errors from the median and quartile estimates. Therefore, further subdivision should be used with caution.

The extreme, median, and quartile values are recorded on probability paper using either probability or cumulative probability distributions for this report cumulative distributions are used. Figure 5.9 is a description of the points chosen. A curve fit may be drawn (or generated on a computer) for the points as shown in Figure 5.10.

(d) One may wish to derive discrete probability assessments from the curve fit shown in Figure 5.10. Given a continuous probability distribution, the distribution is distinguished into probability intervals shown in Figure 5.11. The number and sizes of the intervals are at the discretion of the user. Horizontal lines are drawn crossing through the curve. The break points for the values are at B, D, and F. Within the interval [0,B] a vertical line is moved until the shaded areas are equivalent in size. The value associated with the equivalent areas, A, is recorded as the value associated with probability p_1. The process is repeated for intervals [B,D] and [D,F]. The final outcome is equivalent to the discrete probability distribution shown in Figure 5.12. The probabilities and associated values are input into the variables of the influence diagram model.

5. *Verification*:
There are two parts to the verification procedure. First, the cumulative distributions generated by the encoding process is used as a means of feedback in determining if the distribution is consistent with their judgments. This verification method is important for examining probabilities in the extreme values ranges (see Figure 5.9; value intervals $[0,v_1]$ and $[v_5, \infty)$). Second, is to choose a sequence of value pairs to determine if the values would be equally attractive. This is accomplished by using

the method described in the preceding section for determining median and quartile values. Additional values are chosen lying between the median and quartile intervals to determine if the curve is consistent with experience and judgment. This process should be performed 3 to 5 times to acquire confidence in the curve.

Human Factor Safety Index Method (HESIM)

See Chapter 5. and Appendix 3.

SENSITIVITY ANALYSIS

Sensitivity analysis are performed on both decision and state variables. The following procedure describes the methods used for sensitivity analysis on decision variables and state variables.

(a) After developing the influence diagram model representation (see Section 4.3.3) the influence diagram and remove all variables which may be eliminated through heuristic judgment.

(b) Fix all the nominal values for state variables (probability variables) in the model. The values nominal values may be obtained through the probability encoding procedure methods described above, the HESIM, casualty data, or other valued sources.

Decision Variables

(c1) Determine the sensitivity of the final outcome to the variability in decisions. This is accomplished by using the influence diagram program *InDia* and is further described in Appendix 4.

(d1) Retain the decisions whose variability has substantial impact upon the outcome of the model. Delete the decisions from the model which have only small effects on the overall outcome.

State Variables

(c2) Determine the sensitivity of the final outcome to the range of possible values in state variable similar to (c1).

(d2) Retain the state variables whose variability has substantial impact upon the outcome of the model. For state variables, it is not necessary to delete the variable from the model if the impact is negligible. The variable may be made deterministic by leaving it at the original nominal value chosen.

HOE DATA COLLECTION

The following steps provide a framework for how data should be collected:

The following is a procedure by which to collect and document HOE's for marine casualties and near misses. The procedure incorporate

(1) *Identify the class of accidents for which the casualty data is to be collected* (e.g. collisions, groundings, offshore production fires or explosions, crane

accidents, etc.). Separate database are collected for each accident class of interest.

(2) *Identify casualties by the degree and type of consequences.* This may be established by first identifying what are considered "small", "nominal", "large" and catastrophic consequence levels and categorize consequences on this basis. The consequence levels are identified at the user's discretion. In addition, the user identifies the intervals of consequences for which data is compiled.

(3) *Establishing the stage of occurrence of contributing factors to the accident or near miss sequence.* The casualty stages: underlying or contributing, direct, and compounding were discussed in Chapter 4. It is the responsibility of the user to define underlying direct, and compounding stages to assure error data is categorized into the appropriate casualty stage (see case study examples in Section 7.2).

The HOEDQS provides a format for the user to first identify a *primary* EDA at each accident stage. In addition, the user has the option of including *associated* accident events, decisions, and actions. Associated EDA's are relevant to the primary EDA (see tanker collision-grounding model in Section 7.1).

(4) *Determine contributing human factor, system and task complexity factors related to the event, decision, or action being performed.* For each EDA there could be related human factors, task, or system complexities that contribute to the casualty. In the HOEDQS, the user has the option of including human factor, task, and system complexity to the database (see Chapter 5 and Appendix 3).

(5) *Establish the environmental impairment contributor associated with the event, decision, or action that may have induced human and organizational errors.* Each external and internal environmental impairment contributor presented in Table 3.1 is included in the HOEDQS program allowing the user the ability to input that factor as an error contributor.

(6) *Identify the contributing top-level management factors for the event, decision, or action performed that may have had a direct impact upon human and or mid-level/front line management errors.* The HOEDQS user has the option of inputting their assessment of the impact of TLM factors on the accident scenario (see Section 5.6). Top-level management factors measured are overall commitment to safety, commitment to long term safety goals, cognizance of operational problems, competence to address the problems, and sufficient resources assigned to safety issues to correct problems.

(7) *Identify the contributing human and organizational errors at each stage of the accident sequence and relative certainty of joint human error and mid-level/ front-line organizational error occurrences.* The joint occurrences are defined as the influence between a front-line operator error (HE_i) and an organizational error (OE_j) for the EDA under the task, system, human factor, and environmental conditions. As a result of the complexity of any accident or near miss event, the HOEDQS allows the user a level of flexibility in associating the joint occurrences of human and organizational errors. The user is allowed to input whether they believe there is a "high", "moderate", or "low" certainty of joint occurrence of a particular HE and OE. When

inputting accident data the following guidelines for determining error certainty levels are as follows.

(i) *High certainty of joint occurrence*: The accident/near miss investigator has direct proof or evidence of the incidence of a particular HE occurring at the front line level as a result of a particular MOE.

(ii) *Moderate certainty of joint occurrence*: The accident/near miss investigator has reasonable proof (direct or indirect) of the incidence of a particular HE occurring at the front line level as a result of a particular MOE.

(iii) *Low certainty of joint occurrence*: The accident/near miss investigator has indirect proof or limited reason to suspect an occurrence of a particular HE at the front line level as a result of a particular MOE.

EVALUATING HOE MANAGEMENT ALTERNATIVES

Considering HOE Management Alternatives

Reducing the frequency of errors (prevention) and consequences (mitigation) are the primary focus of HOE management alternatives. The goal is to provide cost effective HOE management alternatives that effectively reduce HOE's at the operator level. Costs in resources to an organization to implement HOE management alternatives can be in finances, time, and expertise devoted to operational safety of a system. The reduction of the frequencies of errors and consequences are generally accomplished in three ways:

(1) *Development of HOE management programs.* The programs specifically address particular error types or error inducing activities. The programs target HOE's at each level throughout the organization such as training, incentives, communication and information systems, safety enhancement programs, and regulating and policing. Error management programs would most likely have indirect effects on reducing other HOE's. Expert judgment is required in estimating these types of indirect effects.

(2) *Change in operating procedures.* The operating policy and procedures indirectly affect HOE's particularly at the operator level through changes in: maintenance programs, greater redundancy and robustness of operation, increase (or decrease) manning requirements, and job design.

(3) *Development of human error tolerant (fail safe) systems.* Heuristic judgments or experiences from similar industries can be used to assess the effects of the management programs upon particular contributing errors.

Factors in Modeling HOE Management Alternatives

Safety Management Programs

Safety management programs (Alternative 1) primarily affect modeling process by direct reduction of the probabilities of human errors at the operator level. The potential reduction of errors may be assessed by:

(1) *Comparison with similar industries in HOE management programs.* Training programs are required in operations of high risk industries such as nuclear power facilities and chemical and hydrocarbon processing plants. The comparison allows decision makers to examine the reduction of error frequencies. Alternatives of management programs are evaluated to determine which are the most effective for the unique operating conditions, management factors, and regulatory environment.

(2) *Use heuristic judgments to determine the direct and indirect effects of the HOE management programs upon organizational and operator errors.* Judgments and experiences of experts are used to determine the impact of HOE management alternatives by using the probability encoding methods and the HESIM both described in Section 5.6. The experts would arrive at their best judgment as to quantitative impacts of management alternatives on the contributing HOE's (see examples in Chapter 7).

(3) *Continuous collection and assessment of human error data to monitor impacts of error management systems.* Direct data analysis is the most effective method of determining HOE management programs. An HOE data collection procedure is described in Section 5.7.1. As the data is collected and updated, the effects of management alternatives are measured with a greater level of accuracy (see Section 5.7.2).

In Chapter 5 we introduced a human error database system, the HOEDQS, that allows users to monitor the effects of particular types of human errors in accident scenarios. As described in Chapter 3, safety management systems are in a constant state of change in unison with changes in the organization. It should be realized that an organizations resistance to safety problems is also in a constant state of change. The HOEDQS is a tool that can assist users in monitoring both trends in casualties near misses and assessing the impact of HOE management alternatives once implemented.

CRITERIA FOR MAKING HOE MANAGEMENT DECISIONS

See all of Chapter 6.

Appendix 5:

Related publications by authors

Society of Naval Architects & Marine Engineers
Northern California Section
Student Paper Presentation
April 9, 1992

The Grounding of *Exxon Valdez*: An Examination of the Human and Organizational Factors

by
William H. Moore, Student Member
Department of Naval Architecture & Offshore Engineering
University of California at Berkeley

Abstract

Just after midnight on March 24, 1989 the tankship Exxon Valdez ran aground on Bligh Reef in Prince William Sound, Alaska. The consequences of the accident was the loss of 258,000 barrels of crude oil resulting in substantial environmental and economic loss. The vessel possessed the best technology available in the tanker industry and was the pride of the Exxon fleet. However, the complexity and the potential catastrophic consequences of using these new technologies is leading us to examine a more critical element: the human factor.

It has been determined that approximately 65% of catastrophic marine related accidents have been the result of compounded human and organizational errors (HOE) during operations. Consequently, tanker operators and regulatory agencies have begun to realize the importance in examining the critical human factor element in tankship operations. Probabilistic risk analysis (PRA) procedures using influence diagramming are currently being developed to examine the effects HOE in marine related accidents.

This paper examines: (1) the human and organizational elements which led to the grounding of Exxon Valdez, (2) structuring of the accident cause-effect relationships into an analytical framework, (3) methods for probabilistic risk analysis (PRA) of HOE in the accident, (4) changes in operational and regulatory policy in post-Exxon Valdez era, and (5) methods for determining HOE management alternatives for future tanker operations.

Introduction

Just after midnight on March 24, 1989 the tankship *Exxon Valdez* ran aground on Bligh Reef in Prince William Sound, Alaska. Within the next 24 hours, the tankship spilled 258,000 barrels of oil into Prince William Sound. The vessel possessed the best technology available in the tanker industry and was the pride of the Exxon fleet. Nevertheless, the grounding led to the worst environmental and economic tanker oil spill in U.S. history. It has been stated that the Exxon Valdez had run aground on Bligh Reef the day oil was discovered on the Alaskan North Slope such that a catastrophic oil spill in Prince William Sound (PWS) was an accident waiting to happen. It just so happened to Exxon before anyone else.

This paper examines: (1) the human and organizational elements which led to the grounding of *Exxon Valdez*, (2) structuring of the accident cause-effect relationships into an analytical framework, (3) methods for probabilistic risk analysis (PRA) of HOE in the accident, (4) changes in operational and regulatory policy in post-*Exxon Valdez* era, and (5) methods for determining HOE management alternatives for future tanker operations.

Background

The events surrounding the accident has brought to surface a critical element in tankship operations: the human factor. Historically, engineers, operators, and regulators of marine systems have looked toward "technological fixes" to reduce the chances of accidents. Only after the grounding of *Exxon Valdez* have we looked to address the human element since sufficient technology was available to prevent the accident from occurring. Approximately 65% of all catastrophic marine related accidents are the result of

compounded *human and organizational errors* (HOE) during operations [1, 2].

In a world of increasing technological growth, society has looked at the benefits of new technologies and the seemingly endless opportunities in their use. However, accidents such as *Bhopal*, *Three Mile Island*, *Chernyobl*, and *Piper Alpha* disasters have led us to realize our limited understanding of complex technological systems and reassess the potentially catastrophic consequences of high technology disasters [3]. Two major factors are involved in analyzing these "high consequence - low probability" accidents: (1) the complexity and limitations of the technological systems were not well understood by the operators (latent flaws leading to catastrophic consequences, excessive reliance on technology), and (2) human and organizational elements were major contributing factors (individual errors, lack of information and incentives).

As engineers, operators, and regulators of potentially catastrophic systems, it has become critical to directly consider the effects of HOE on tanker operations in reliability based analysis. Currently there is no structured quantitative approach to assist engineers, operators and regulators in addressing HOE factors in tanker operations. Qualitative (social and management issues) and quantitative should be used concurrently to address HOE factors. Qualitative analysis should be used as a framework for quantitative analysis [4]. One method of examining HOE related factors in accident scenarios is through the analysis of case history examples. Well documented case histories can give valuable insight into the interaction of causal factors over an extended time (contributing, direct and compounding HOE's) [5].

Established HOE quantitative analysis methodologies for tanker and offshore platform operations are currently being researched through a joint-industry project, *Management of Human Error In Operations of Marine Systems* in the Department of Naval Architecture & Offshore Engineering at the University of California, Berkeley. In the first year of the project, the effort was directed at identification, acquisition, and analysis of well-documented case histories and databases of high consequence tanker and offshore platform accidents whose root causes are founded in operations HOE. Current focus on the second year of the project has been to develop an organization and classify (taxonomy) the sources of HOE, and to develop data bases that can be used to quantify the rates of HOE. An analytical framework is being developed that will allow evaluations of the interactions of HOE errors in causing accidents. In the third year of the project, the effort is to be directed at the verification of the quantitative analyses, and development of examples that will demonstrate the effectiveness (costs and safety benefits) of various alternatives to reduce incidents of high consequence HOE.

The *Exxon Valdez* is being used as a tanker case study example (the *Piper Alpha* disaster is a case study example for platforms). The current status of the research is in the developments of the analytical framework models. Quantitative analysis of the accident will be conducted within the following months.

The grounding of *Exxon Valdez*

The events described surrounding the grounding of *Exxon Valdez* have been taken primarily from the National Transportation Safety Board Report (1990) and National Transportation Safety Board Factual Reports (1990). The events described primarily focus upon the actions of the *Exxon Valdez* crew, the Vessel Traffic System (VTS) crew, and the pilot.

Captain Hazelwood had been off the ship during the day she was loading crude oil in Valdez. By his own confirmation he was drinking that day. The NTSB's proposed findings of the facts conclusions and recommendations states, his blood alcohol level would have been approximately .285 at the time he boarded the ship, to do so without showing some evidence of physical impairment or needing some assistance. Additionally a cab driver and an Alyeska guard interviewed by the Board investigators reported none of the *Exxon Valdez* crew members returning to the vessel were "under the influence of alcohol". During the time the pilot was aboard the ship, the pilot smelled alcohol on Captain Hazelwood's breath. He had been off of the bridge for approximately one hour and thirty-five minutes before returning at the time of the departure of the pilot.

Late on March 23rd, shortly prior to his relief, the helmsman responded to an order from the master to sail the ship 180° and put her on automatic pilot. Helmsman Harry Claar was puzzled by this order. He didn't check it with the master. The master left the bridge but not before asking the third mate, Cousins, if he felt comfortable sailing the ship under these conditions. Despite his limited experience in sailing the ship, he replied that he did. Federal and Alaska state law require that ships be under the control of a federally licensed pilot when transiting in U.S. pilotage waters (inside the three mile territorial seas).

At 2347 the ship left the Traffic Separation Scheme (TSS) going into the inbound lane to avoid the ice. At 2355 the helmsman was relieved by Robert Kagan [6]. The NTSB has simulated the path which *Exxon Valdez* traveled once deviating from the TSS and is

shown in Figure 1. The ship was on "load program up" which meant she was increasing her speed while exiting the harbor. Thus, *Exxon Valdez* was traveling at 12 knots and on automatic pilot just prior to hitting Bligh Reef. Putting the ship on automatic pilot in confined waters and not telling the third mate the master had done so was extremely inconsistent with normal practice. At his relief at 2350, the helmsman reported to the third mate that the ship was on automatic pilot, something the third mate did not know about (there is some speculation that the ship was operating on automatic pilot until the grounding). The third mate did not discuss the reason for the automatic pilot with the master.

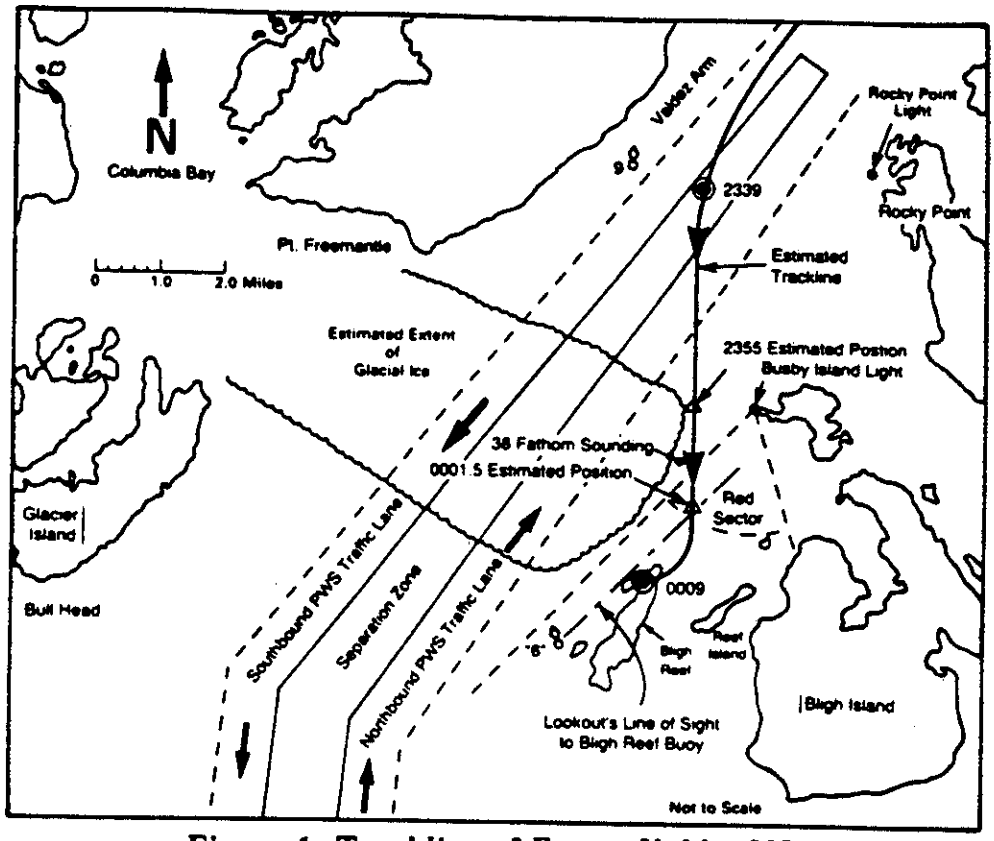


Figure 1: Trackline of *Exxon Valdez* [9]

The third mate was Gregory Cousins. He holds a second mate's license, and first sailed as the third mate on an Exxon tanker in January, 1987. He had sailed on five tank vessels owned by the company and had been employed by Exxon for nine years. He had completed approximately 18 voyages in and out of Valdez, sailing in both unlicensed and licensed categories. At the time of the grounding he had approximately 199 days of at sea experience as a third mate.

The night before he slept from 0100 to 0720, then after lunch had a cat nap (1300 to 1350) and relieved the chief mate for supper and worked through to the grounding. The third mate had only about a year's experience as a deck officer. The situation is further complicated because the chief mate had worked the entire time of the loading, was asleep, and was unavailable as an additional resource. In addition to his bridge duties, the cargo is the primary responsibility of a chief mate in the Merchant Marine. This includes loading and discharge of cargo could only be conducted by the second and third mate on duty, the chief mate is normally on hand for loading and discharging are initiated and concluded. The ship left port at about 2054.

The third mate decided not to call his relief, the second mate, until after they cleared the ice (the error might have been detected through the watch relief procedures). The third mate determined there was .9 mile between Busby Island and the ice floe and felt he could pass around the ice. The master left the bridge at 2352. The third mate relied considerably on the radar, but did not correlate the radar information with

the navigation charts through position fixing. The submerged reef was not displayed on the radar.

Watch condition C (Exxon Bridge Organizational Manual) stated that two officers be on the bridge during this transit. The chief mate was sleeping. Some time before 2355 the third mate put the ship on manual control. At 2355 he plotted the ship as 1.1 miles from Busby Island. Before midnight the AB reported a red light flashing every five seconds to the third mate. He acknowledged her and stated that he knew the light to be Bligh Reef, light #6. The third mate ordered a right 10 degree rudder but the vessel did not move to this position. There is a six minute delay before the third mate and helmsman respond to the fact that the ship did not begin to turn. The Kings Point simulation of the exercise shows the helmsman could have turned the rudder 10 degrees and shortly thereafter inadvertently moved it to four or five degrees. The third mate might well have failed to detect such an error for six minutes.

About this time the AB reported the light flashing every 4 seconds on the wrong side of the ship. Now the third mate orders a right 20 degree rudder. Moving at 12 knots while the ship was still engaged in maneuvering evolutions to avoid ice violated prudent ship handling practices while increasing risk of damage to the ship if ice floes had been struck. He then orders hard right rudder. The third mate testified that two officers normally served on the navigation watch when Exxon vessels were maneuvering in confined or congested waters.

When the vessel struck the reef, the third mate ordered a hard left rudder to get the ship to stop swinging to the right and prevent the stern from swinging around. The ship had clearly skidded into Bligh Reef. The helmsman was confused about some aspects of the situation. He also reported that the third mate was panicky. The chief engineer stopped the engines at 0020. It's not clear from the NTSB report what time the ship hit the reef, but the engineer acts as if he stopped the engines after the ship hit. It's possible the ship didn't stop until 0090. At 0027 the master lets VTS know the ship had run aground and at 0035 the master ordered the main engine restarted.

For approximately 45 minutes the master made an attempt to remove the vessel from the reef, probably moving from dead slow ahead to full ahead, and finally slowing down and stopping. The chief engineer had advised the master not to move the ship. VTS had advised to move cautiously.

Exxon states that Hazelwood was not trying to dislodge the ship from the reef because he never put the ship astern. According to NTSB documentation the record fully supports the fact that Hazelwood gotten the ship off the reef it would have capsized. Other evidence suggests it might not have [7]. However, Captain Deppe, Exxon Shipping spokesperson, testified that only the support offered by Bligh Reef kept them afloat. VTS had advised to move cautiously. XO and Senior Investigating Officer (SIO) from the CG Marine Safety Office (MSO) boarded the ship at 0335.

VTS involvement the night of grounding

The lack of vigilance with which the VTS handled operations the night of the accident is another factor in the grounding. Only one civilian watchstander and one enlisted radioman were on duty. But the accountability and responsibility rested with people who weren't there. Neither the Commanding Officer (CO) nor the Executive Officer (XO) were at the VTS. The VTC manual requires the watchstander to advise the Officer on Duty (OOD) when a vessel deviates due to ice in the lanes. The 1600 to 2400 watchstander failed to do this. The 1600-2400 watchstander said he believed the radar didn't detect *Exxon Valdez* because it wasn't working properly. However, he did not report a malfunction to his relief or the electronics technician on duty. The watchstander's relief came on at 2333, and checked things out. Neither watchstander was aware that *Exxon Valdez* had altered course from 200° to 180°. *Exxon Valdez* was lost on the radar but could have been acquired. The 0000-0800 watchstander said he didn't try to do this because he'd been told by the other watchstander that the *Exxon Valdez* was no longer visible on radar. At the time of the accident the watchstander was away getting a cup of coffee. That the radar was operating appropriately is evidenced by the fact that the watchstander had no difficulty detecting the grounded ship.

The ship previously leaving the port reported heavy ice to the VTS but the VTS saw no reason to report this to *Exxon Valdez* or to more carefully monitor her. At about 1930 a passenger ship approached Valdez. Her captain said the ice was some of the worst he had ever seen and reduced speed. He did not report this to the VTS. At 1930 the outbound *Arco Juneau* reported ice in the TSS. The VTC operator said he was concerned about the heavy ice reported by the *Arco Juneau* but that didn't motivate him to have the ship report her position more frequently, nor did he report that to the *Exxon Valdez*. Both ships transited during the day and neither had as far outside the TSS to go as the *Exxon Valdez* because when she transited the ice was much further to the northeast.

The ship previously leaving the port reported heavy ice the VTS but the VTS saw no reason to report this to *Exxon Valdez* or to more carefully monitor her. At

about 1930 a passenger ship approached Valdez. Her captain said the ice was some of the worst he had ever seen and reduced speed. He did not report this to the VTS. At 1930 the outbound *Arco Juneau* reported ice in the TSS. The Vessel Traffic Center (VTC) operator said he was concerned about the heavy ice reported by the *Arco Juneau* but that didn't motivate him to have the ship report her position more frequently, nor did he report that to the *Exxon Valdez*. Both ships transited during the day and neither had as far to go outside the TSS as the *Exxon Valdez* because when she transited the ice much farther to the northeast.

Exxon Valdez remained on course 180° for nearly 18 minutes. The VTC operator had ample time to call the vessel and ascertain her intentions. Any inquiry from the VTC regarding the vessel's intentions probably would have alerted the third mate to turn earlier or apply more rudder. The VTS communication system failed to meet the Coast Guard's requirement of 99.9% operational status. During the evening of March 23rd the Naked Island and Cape Hinchinbrook remote communication sites were inoperable. The system was old, requests for money had been denied, and the harsh Alaskan climate degrades the system easily.

Only when *Exxon Valdez* called the VTS did the watchstander know she had gone aground. He then adjusted the radar and picked her up. There's a lot of testimony about how watchstanders thought the radar wasn't working well. The number 1 (master) radar which synthetically displayed the TSS boundary lines was burned out. The Coast Guard was warned in 1984 that the system would begin deteriorating in the next two years without attention. After the accident the Operations Officer testified that he noted its deterioration in the last two years. The contractor didn't keep the system well maintained and as a result it was inoperable up to 28% of the time.

The human and organizational elements

The human and organizational contributions can be separated into: (1) underlying factors creating a reduced tolerance of the state of the system (primarily the organizations) and (2) actions by the front line operators (primarily the individuals) whose errors initiate the catastrophic events [5]. The underlying contributors were Exxon Shipping Company and the U.S. Coast Guard. The initiating contributors were the crew aboard the vessel and the VTS crew stationed in Valdez. The failure of these individuals in preventing the accident can be attributed to both individual errors by the tanker crew and VTS personnel. In addition, the Exxon Shipping and the Coast Guard played contributing roles in establishing an operation which had few checks and balances to maintain safe tanker operations. The system had atrophied through the years and little effort had been put forward to maintain reliable operations [8].

Exxon Valdez crew

The NTSB concludes that considerable uncertainty remains concerning the master's intentions for maneuvering the vessel back toward the Traffic Separation Scheme (TSS). The master would have to begin turning back into the lanes when he was abeam Busby Light. However, both he and the third mate noted on the chart a position about 7/10 of a mile further to begin the turn. By making the turn abeam Busby Light the ship would have drifted about a half mile further but then would have come parallel to the lane. By advancing further the navigational maneuvering required to bring the ship back into the lanes was considerably more extreme. The board concluded that it was feasible to begin the turn either abeam Busby light or 7/10 of a mile further south, as long as the watch was capable of simultaneously monitoring the vessel's position relative to Bligh Reef, watching out for ice, and conning the vessel.

"The frequent fixing of the vessel's position could have taken a substantial amount of the third mate's time and would have limited his ability to concentrate on other important functions, such as watching for ice and conning the vessel. Conning also requires careful supervision of the helmsman. Under normal conditions, when a master or a pilot is conning the vessel, the watch officer assists by carefully observing the actions of the helmsman in response to orders from the master or pilot. This enables the officer conning the vessel to concentrate on observing and directions the vessel's movements. In this instance, the helmsman had limited steering experience and required additional supervision. The master was aware of the helmsman's limitations and should have considered them before leaving the bridge [9]."

Testimony given the investigating board indicated that there could be a period of 20 minutes when no lookout is posted. This period is caused then the lookout and helmsman change assignments. In this instance there is no evidence that the lack of a lookout from 2340 to 2350, when the AB assumed her lookout, contributed to the accident.

Exxon Shipping Company

Several operational policies and procedures of operations of Exxon Shipping Company were observed to have potentially contributed either directly or indirectly to the accident:

(1) Reduced manning levels led to fatigue and job overload.

(2) There were no established policies regarding procedures to reduce the risks of operating with smaller crews.

(3) Lack of compliance with federal statues regarding work schedules for deck officers.

(4) Tanker crews had not complied with written company policies regarding drug and alcohol internal policing to ensure compliance.

Reduced manning in the U.S. merchant marine fleet has become a high profile issue in both the domestic and foreign the maritime industries. The industry and regulators have conducted, funded, and participated in studies to determine the cost and effects of reduced manning. Many of these studied have been conducted to justify crew reductions to cut operating costs. The policies Exxon Shipping Company had in updating fleet and reducing crew are consistent with those of the industry.

Yet, there is no evidence Exxon Shipping Company had policies or procedures to examine the risks and reliability of using reduced crews. No supervisory training recognized such factors as fatigue, social isolation, longer hours at sea, etc. There was no company program to monitor officer's work in excess of eight hours a day. There was evidence that officers now did deck work that unlicensed workers do before the accident.

In June, 1988, Frank Iarossi (former president of Exxon Shipping) presented a paper titled "Surrendering the Memories" in which he stated that it was Exxon's policy to reduce its standard crew compliment to sixteen by 1990. He noted that other ships (mostly foreign flag) successfully operated at such levels. The paper focuses on economic issues yet makes little mention of considerations of ship safety and crew fatigue. The NTSB came to possess three memos to Exxon Shipping Company masters ordering them to purposefully reduce overtime to satisfy Coast Guard overtime concerns and to better argue for reduced manning levels.

Reduced manning may certainly have led to Exxon Shipping Company's failure to comply with two federal statutes regarding work hours for deck watches. The first states that an officer cannot take charge of the deck watch on a vessel when leaving a port unless he has been off duty for at least six of the twelve hours immediately before leaving. The second states a licensed individual or seaman is not required to work more than eight hours a day except for safety related functions (the average workday was approximately 10 hours including voluntary overtime). Apparently Exxon Shipping Company had no provision for giving six hours of rest to any deck officer before getting underway.

It appears that company's written policies about alcohol and drug use weren't taken very seriously. The policy instructs supervisors to report to the medical department employees whose performance was unsatisfactory due to alcohol use. Crew members are not to perform job duties within four hours of having a drink. Hazelwood entered an alcohol rehabilitation program in 1985 which the company learned about when his supervisor tried to contact him. No supervision was involved in making sure he continued with some sort of support group. The disability began April 1, 1985 and ended on May 16, 1985 and was followed by a 90 day leave of absence. Captain Hazelwood then returned to sea duty. The NTSB concludes that he should have been confined to shore duty until there was ample proof this problem was under control. After the leave of absence the fleet manager and ship coordinator were given follow up responsibility including visits to his ship.

Captain Hazelwood's performance evaluation of 1988 had been more than satisfactory. Yet he had two convictions for DUI (1985, 1988) and had a suspended drivers license at the time *Exxon Valdez ran* aground. Annual performance appraisals for the masters were not available for every year. The company has made no statement about how it follows up on appraisals. A number of statements about Hazelwood's performance lead to the conclusion that he had difficulties managing people as early as 1974 [9].

U.S. Coast Guard

Three Coast Guard HOE factors are observed to be contributors to the accident.

(1) Supporting (whether voluntarily or involuntarily) the reduction of crew sizes leading to fatigue and job overload.

(2) Deterioration and downgrading of the VTS in Valdez over the years.

(3) Reorganization, loss of billets, and use of inexperienced personnel for VTS duties in Valdez.

Vessel Manning

Reductions in vessel manning requirements has become a increasingly controversial topic of debate. The controversy is fueled by operators using reduced crews for foreign flagged vessels not under U.S. Coast Guard jurisdiction. The Coast Guard currently depends on an integration of laws, regulations, informal policy guidelines and maritime tradition to establish guidelines for crew manning levels [9]. The Coast Guard earlier concluded that minimum manning for the vessel would be fifteen crew members (*Exxon Valdez* had 20 crew members when she grounded on Bligh Reef). Events aboard *Exxon Valdez* indicate

that fatigue and job overload had led to the chief mate not being present on the bridge while transiting PWS as would his normal duties dictate. The presence of the chief mate may have led to better decision making while in transit. In addition, the presence of an additional mate on the bridge could have added to the redundancy of the bridge watch.

Vessel Traffic System (VTS)

In 1971 the Coast Guard developed preliminary concepts for VTS and in 1973 submitted a final VTS study report estimating there would be a reduction of approximately 70% of the accidents caused by collisions, rammings and groundings. In 1977, the U.S. Coast Guard VTS systems were being planned and operated in San Francisco, Puget Sound, New York, New Orleans and Berwick Bay, Houston/Galveston, and Prince William Sound (PWS).

In 1988, Coast Guard fiscal budget constraints resulted in the closure of both the New York and New Orleans VTSes. In a report to Congress, the General Accounting Office issued a report stating that the Coast Guard had chosen both New York and New Orleans VTSes: "to resolve it's immediate problem of reducing operating expenses and gave little consideration to the effectiveness of each of the VTS's in enhancing safety." [11]. This general lack of importance manifest itself in the deterioration of the VTS in PWS over the ensuing years.

Before VTS was established for PWS in 1977, marine safety functions were conducted by the Marine Safety Detachment (MSD) under the authority of the MSO Anchorage. When the MSO was established in Valdez, additional duties were taken on which had normally been performed by the MSO Anchorage. Unlike other VTSes across the country, Valdez VTS personnel could be utilized in non-VTS duties at the discretion of the Commanding Officer (CO). This gave the green light to the CO MSO Valdez to distribute MSO duties as he wished. In a letter to the CO of the USCG headquarters in 1985 he stated, "...what MSO Valdez does much larger than just having a few people watch radar screens in the least-trafficked, yet fully federally mandated, VTS in the country" [9].

The VTS consisted of a Vessel Traffic Center (VTC), radar surveillance system, and a communication system. The VTC is manned 24-hours around the clock by two watchstanders (one radar watchstander and one radio watchstander). The radar watchstanders responsibilities were to maintain vessel positions while the radio watchstander established and monitored radio contact for PWS. The radar surveillance system had initially been able to maintain contact with vessels from Port Valdez to areas south of Bligh Reef. Vessels were required to give VTS general information about vessel name, position, estimated time of arrival (ETA) to navigation in VTS area, speed, cargo type, towing, vessel impairments, and additional requested information three hours before entering PWS. Once in VTS waters vessels were required to report speed changes, intentions of crossing the TSS 10 minutes prior to crossing, when clearing the Traffic Separation Scheme (TSS), and when vessels pass a reporting point.

One obtains a picture of a deteriorating service over the years preceding the accident. A greater burden had increasingly been placed on the commanding officer to engage duties not directly related to VTS. Monitoring procedures were changed and became less rigorous over the years. When the VTS was installed in 1977 the watchstander plotted the range and bearing of all vessels transiting the part of the port under radar control. In 1984 new Raytheon equipment was installed and plotting was discontinued. This change wasn't noted in writing until 1987. The 1987 memo was issued because the dramatic increase in shipping traffic was placing too many burdens on the operators. The memo was designed to reduce work associated with vessels in Valdez Arm. Vessels transiting Valdez Arm were to be monitored, but no written guidance about how far to monitor outbound traffic or when to acquire inbound traffic. This was left to the discretion of each watchstander.

VTS was a part of the Operations Department and performed duties other than watchstanding. Watchstanding had been reduced at the same time that the potential for problems due to ice floes in the sound was increasing. Procedures for certain eventualities were not well spelled out or implemented. In addition, it appears the current CG CO had not put the pressure on his superiors to upgrade equipment in the way his predecessor had done.

The VTS was reorganized in 1982, making four of the five watch supervisors department heads who had little to do with supervising watches. In 1986 the CO of MSO Valdez proposed that MSO Valdez be downgraded to a MSD. The proposal also eliminated five VTS officer watchstander billets. In 1987 the watches were discontinued and replaced by a Command Duty Officer (CDO). The CDO was not required to be at the VTS during routine vessel transits. However, it was required that he be contacted in the event that vessels deviated from the TSS. The CDO could be contacted 24 hours a day if conditions arose where vessels need to deviate from the traffic scheme.

In 1988 the VTS lost five billets. As a result remaining personnel took on additional functions having little to do with VTS and by default the senior watch-

stander became responsible for supervising the day to day operations of the VTS. This person worked days and stood watches when anyone called in sick. In 1988 the OOD and CDO functions were merged and called the OOD and the duties were expanded. Several of the OODs were enlisted personnel, junior to the civilian watchstanders they supervised. On the day of the accident only one OOD was a qualified watchstander. The station OOD on duty prior to the accident had never qualified as a watchstander. Because of the replacement of the CDO with the OOD supervision and communication between the VTC and senior MSO/VTS personnel probably declined. No officer's primary duty was to be in charge of the VTS.

Despite the fact that ships were regularly deviating from the TSS the CO of MSO Valdez reported that if a vessel knows its position and is maneuvering no further radio contact is required. He continued, there is no good reason for a ship to deviate from the TSS, a vessel requesting deviation is requesting something out of the norm. VTC watchstanders don't have the authority to allow vessels to leave the lanes and if a vessel requests deviation the request is forwarded to the Operations Officer (OO) who forwards it to the CO or Executive Officer (XO) for a reply. The fact that neither the CO nor the OO appeared to be aware of the fact that vessels regularly departed the TSS, indicates the data forms were not reviewed to determine routes vessels followed. Since no data were kept there was no standard against which to measure radar or personnel performance.

In 1980, after the *Prince William Sound* lost power and almost ran aground in PWS, the Coast Guard recommended installing reinforced tow lines on the tankers and requiring a tugboat to escort tankers to Hinchinbrook Island. The lines were installed. In 1981, James Woodle, the CO of Valdez, recommended that the Coast Guard radar system be improved in response to the break up of the Columbia Glacier [6]. Nothing was done. In 1986 his successor, Steve McCall, favored downgrading the system. According to the NTSB Report (1990) in 1984 the Coast Guard requested the installation of an additional radar site on either Glacier or Bligh Island. In 1984 the CG and oil companies met to talk about the increasing ice and decided to operate as before. In neither instance was anything done. For a time the oil companies ordered their vessels to operate at reduced speed or only during daylight.

In 1986 the CG issued a series of recommendations and directives that made pilotage so complicated no one knew what was required [6 ,12]. A study done after the accident showed that the existing radar was incapable of reliable radar coverage of Valdez Arm. Through the years, tanker crews became unaware of the extent of the VTS system [12]. In 1988 the CO of the MSO sent the commander of maintenance for the Pacific a letter requesting information on the 1984 request for update. He was notified that as off February 13, 1989 there was no plan for update.

By the early 1980's both the Coast Guard and the maritime industry were concerned about the ice in the sound. Between 1981 and 1984 18.9% of the vessels transiting the VTS area deviated from the TSS because of ice. In August of 1984 a meeting was called between operators, Coast Guard, State Pilots, and Alyeska to discuss ice conditions. A Coast Guard representative makes mention of the true concern of ice conditions in PWS though representatives at the meeting tried to downplay the problem [13]. Nonetheless, an Exxon representative said he was confident in the abilities of the masters and their vessels to handle the situation and would like to see things operate as they were. An Arco representative agreed saying that he believed in preliminary planning reports but no need for further controls. Pilots concurred that the masters would not transit if they felt the ice was too dangerous.

In summer, 1985, a new CO took over at MSO Valdez. He did not require the VTS to keep a record of the number of vessel transits affected by ice. Ice reports provided by the VTC were retransmissions of earlier reports from transiting vessels. Thus, they may well be out of date for the next vessel.

Pilotage

The initial plan of the U.S. based oil companies were to use the pilots for transiting PWS until their masters fulfilled the Federal pilotage requirements. This plan included using docking masters for docking the vessels at the terminals. The Southwest Alaska Pilot's Association succeeded in lobbying and obtaining legislation requiring tankships in excess of 50,000 dead weight tons to employ a pilot while transiting state waters. This law included that the control of the vessel by state or federal pilots during docking thus excluding the use of docking masters. The state pilots each held federal pilotage certification.

In 1977 the state pilot association established a pilot station at Cape Hinchinbrook using a converted fishing vessel, the *Blue Moon*. In 1980 the *Blue Moon* foundered. Due to the dangers involved in embarking and disembarking pilots in the outer Prince William Sound, the pilot station was then moved to Rocky Point at Valdez Arm. At this point, the Alaska Board of Marine Pilots decided not to reestablish the pilot station at Cape Hinchinbrook and eliminated the state requirement for state pilotage between Cape Hinchinbrook and the pilot station at Rocky Point.

The Federal Pilotage requirements still were in effect though there were no transport pilots between Cape Hinchinbrook and Rocky Point.

This created few problems since most TAPS trade masters held pilotage between Cape Hinchinbrook and Rocky Point. However, this did cause some difficulty for the foreign flagged vessels who found themselves dependent upon the pilots for navigating the entire Prince William Sound. Soon after the sinking of the *Blue Moon*, the Coast Guard it was revealed that they had no authority to require foreign flagged vessels from obtaining Federal pilotage. Though the Ports and Waterways Safety Act requiring such pilotage there is no indication that the Coast Guard had established enforcement regulations.

To accommodate the foreign flag tank vessels and U.S. flagged vessels without Prince William Sound pilotage endorsements, the COTP for the Port of Valdez established a set of requirements for transit of these vessels (Port Order 1-80, February 25, 1980). The determination of whether pilotage was necessary was left to the discretion of the duty officer or COTP. The regulations included the limited transit of non-pilotage vessels from Cape Hinchinbrook to the pilot station during daylight hours and two licensed officers on the bridge while transiting the sound (one on watch and the other navigating).

In June 1985, proposed changes in pilotage regulations were introduced (funny that this was soon after McCall arrived on the scene). The Coast Guard reduced the areas of required pilotage. In September 1986, the Coast Guard decided to cancel COTP Order 1-80 and issued requests for pilotage on a case by case basis for tank vessels without pilotage endorsements. The major change was in the requirement of a 2 mile visibility in the sound with potential reassessment of this proposal during averse weather conditions.

After the *Exxon Valdez* ran aground, the pilot station was reestablished at Bligh Reef.

Developing an analytical framework model

Constructing accident analysis framework models involves: (1) structuring the primary events and decisions leading to the grounding, (2) using a human and organizational error classification to determine the contributing causes, and (3) quantitative analysis using either reliable data information and/or expert opinion when reliable data is unavailable.

This analysis follows a progression of modeling stages:

Stage 1: Use influence diagramming structure to establish the dependency of events leading to the grounding.

Stage 2: Establish the accident causes using a human and organizational error classification and model them into the influence diagram framework.

Stage 3: Generate conditional probability distributions using Bayesian statistical techniques from available data sources.

Stage 4: Final construction and evaluation of the influence diagram models to determine overall probabilities of failure and expected returns.

Stage 1: Establishing dependency of events

The model represent the set of events that occurred aboard the *Exxon Valdez*, the vessel transit in and out of the TSS, and at VTC in Valdez. Figure 2 summarizes the dependency of events, direct causes and decisions involved in the grounding discussed above. These influences are represented by nodes, (events, causes, and decisions) and arcs which establish the dependencies. Probabilities are represented by oval nodes, deterministic events are represented by double-lined oval nodes, decisions are represented by rectangular nodes, and expected returns are represented by double-lined rectangular nodes. The development of influence diagram models should be the effort of a group of experts. Discussion of differences in opinion of the relationships of between events and their causes illicit the development of more realistic models [14].

Stage 2: Establishing accident cause

In establishing the accident cause, the first-generation taxonomy being developed for the *Management of Human Error in Operations of Marine Systems* project identifies the contributing causes to marine related accidents:

(1) *human/system interface* (operating environment, normal and emergency control systems)
(2) *knowledge/experience/training* (normal and emergency operating systems)
(3) *maintenance* (normal and emergency operating systems)
(4) *physical/mental lapse*
(5) *violations* (organizational or regulatory procedure or policy)
(6) *morale/incentives*
(7) *job design*
(8) *commitment to safety* (front line operator or organizational)
(9) *regulating/policing* (organizational or regulatory)

(10) *operating policy* (organizational or regulatory)
(11) *communication & information* (operator control system, front line operators, and organizational)
(12) *manning requirements*
(13) *resources* (organizational, regulatory)

The *Annotated Human Factors Taxonomy* (AHFT), soon to be used by U.S. Coast Guard marine casualty investigators, form the basis for the U.C. Berkeley HOE project taxonomy. The AHFT distinguishes underlying, direct, and compounding causes to marine casualty events as exemplified in Figure 3. Additional sources are used to examine *violations*, *commitment to safety*, and *resources*. The influence of causes upon the decisions and events specific to *Exxon Valdez* are shown in Figure 4.

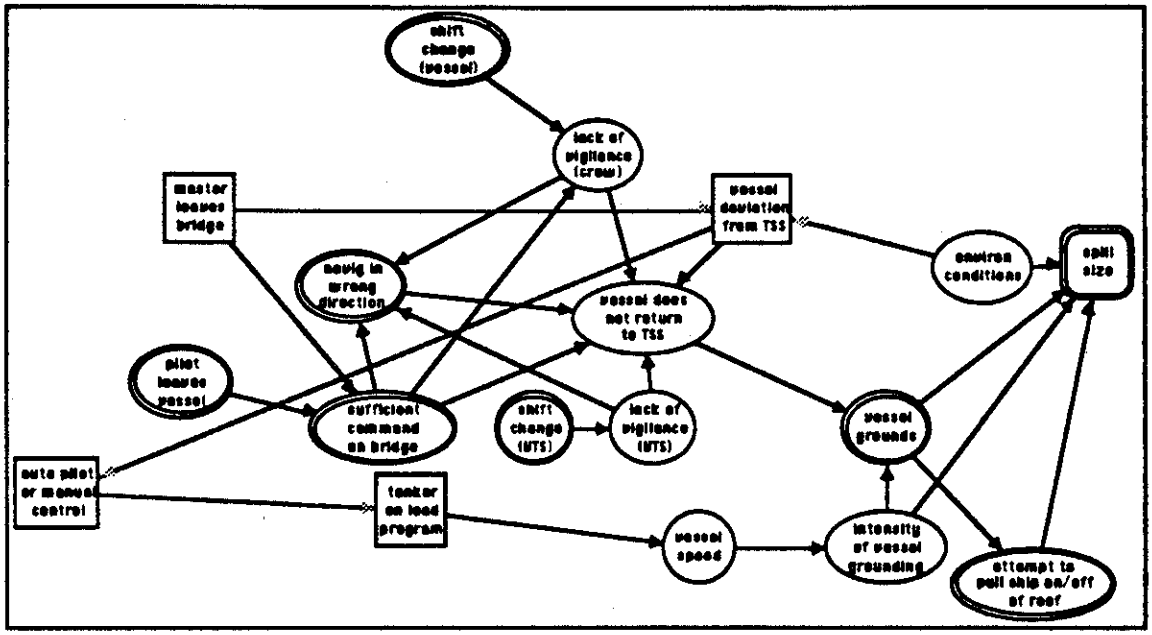


Figure 2: Influence of events and decisions leading to the grounding of *Exxon Valdez*

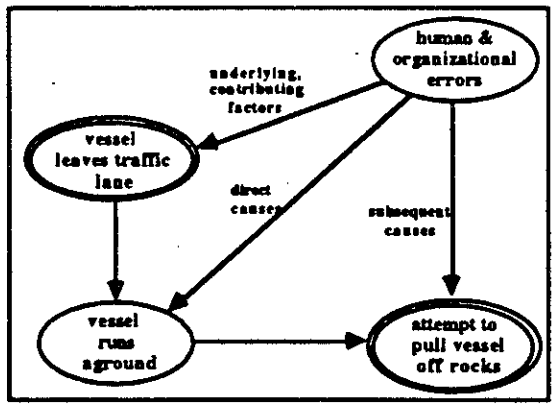


Figure 3: Influence of HOE on sequence of grounding events

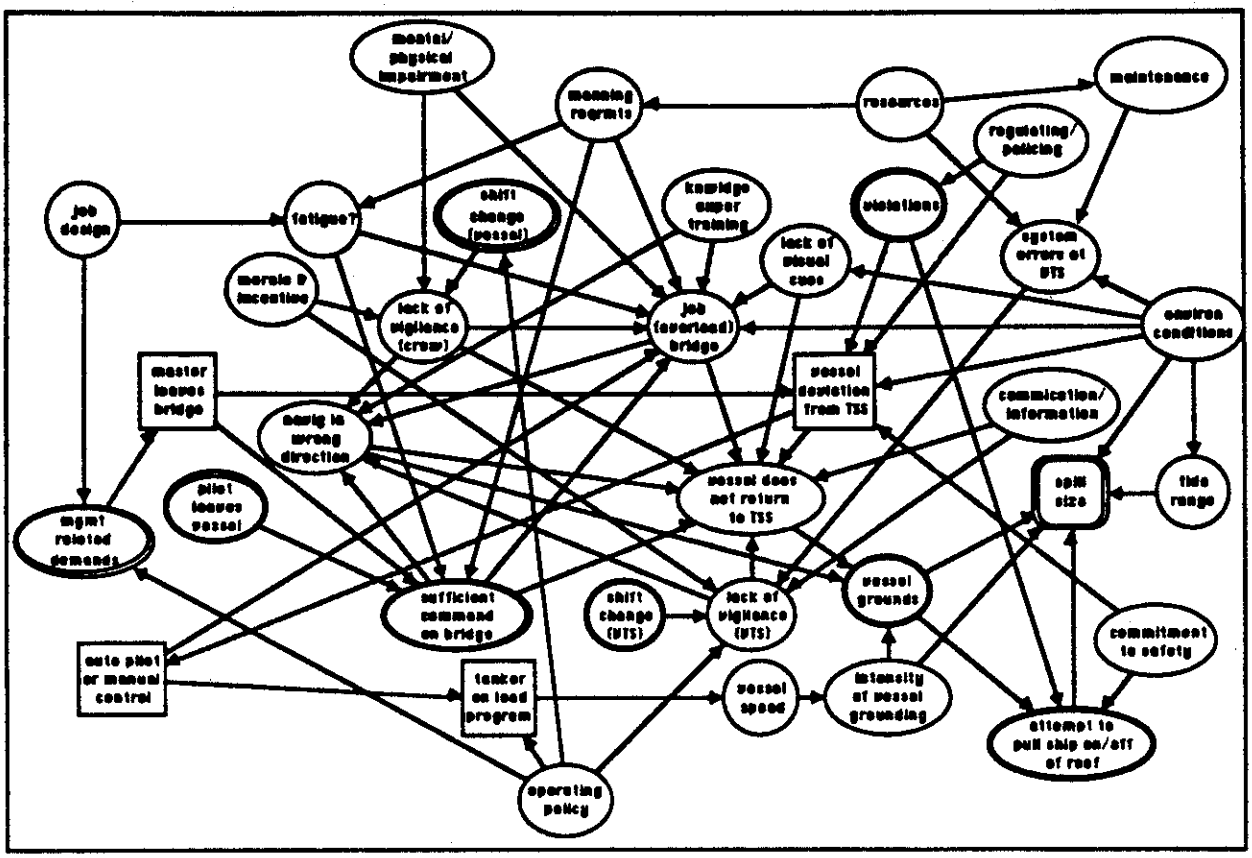


Figure 4: Influence of HOE causes on the grounding of *Exxon Valdez*

Stages 3-4: Probabilistic Risk Analysis

Current quantitative analysis of HOE data is limited to the use of subjective expert opinion. However, computer codes using the AHFT and additional data sources are in the process of development. These codes include the examination of conditional probabilities between events, events, and their causes. Bayes Theorem is used to determine the dependency of events and causes:

$$P(E_i|C) = \frac{P(C \mid E_i)\,P(E_i)}{P(C)} \qquad (1a)$$

$$= \frac{P(C \mid E_i)\,P(E_i)}{\sum_{j=1}^{n} P(C \mid E_j)\,P(E_j)}, \qquad (1b)$$

where E_i is the event or decision i and C is the HOE related cause. Similar relations can be determined between decisions, events and causes. Once the set of conditional probabilities have been established they can be used in the influence diagram models shown in Figure 2 to determine failure probabilities (of grounding) and expected returns (spill size). Dissemination of results of the model calculations are expected in the coming months.

The post-*Exxon Valdez* era

Since the grounding of *Exxon Valdez*, the most influential changes in tanker operations has been the Oil Pollution Act of 1990 (OPA 90). OPA 90 addresses a wide variety of tanker operation issues. These are represent current HOE management alternatives. As an overview, Title IV of OPA 90 [15]:

(1) mandates that the Coast Guard tie into the National Driving Register to detect individuals with drunk driving convictions;
(2) increases Coast Guard authority to deny or revoke mariner licenses and documents;
(3) authorizes removal of incompetent personnel;
(4) increases Coast Guard authority to deny entry of foreign vessels into the U.S. waters on the grounds of deficient manning;

(5) limit crew workhours aboard tankers to 15 hrs/day but no more than 36 hours in any 72 hour period;

(6) mandates the Coast Guard conduct studies on vessel traffic and tanker navigation;

(7) requires all new tanker builds to be double-hulled in addition to the phasing out of existing tankers beginning in 1995 and concluding in 2010; and,

(8) require the Coast Guard to designate areas where two licensed personnel are required to navigate and tug escorts are necessary.

The influence diagram frameworks in Figure 4 can be used to determine the effectiveness HOE related management alternatives of OPA 90 on the overall failure probabilities of the system. Figure 5 summarizes the influences of OPA 90 on the various contributing causes of marine related accidents discussed above. The importance in evaluating are to determine their effectiveness in reducing the overall failure probability of this class of grounding accidents. For example, when legislating OPA 90, was the reduction of cargo capacity of double-hull tankers resulting in more tanker traffic to maintain capacities taken into account [15]? The additional traffic could increase the risk of other classes of accidents such as collisions. It is imperative that these issues are addressed in the PRA analyses framework.

Operational reliability of future tanker operations

There are three primary purposes of conducting post-mortem HOE analysis studies such as the one being conducted on *Exxon Valdez*. First, well documented case histories can give valuable insight into the interaction of causal factors over an extended time. This assists in determining the sources of human errors in various states and stages of accident scenarios. Second, they provide a basis in which to examine the effects of HOE management alternatives of various classes of accidents. Figure 4 provides a basis for a "template" to examine the impacts of OPA 90 and similar existing regulation, policy or operating procedures. Third, general templates are to be formed to examine the impact of a class of accidents similar to *Exxon Valdez*. For example, Figure 6 is a generalized template of the class of grounding accidents. Establishing dependencies between events, decisions, and HOE causes would be at the discretion of the user. Additional nodes and arcs unique to the operating system, environment, procedures or policies are added by the users. The models are then evaluated to determine the overall failure probabilities.

Conclusions

The close examination of the events surrounding the *Exxon Valdez* results in realization of the impact of the human element in a high-technology society. Research and experience indicate that the majority of high consequence, low probability marine accidents have one common theme: *a chain of important errors made by people in critical situations involving complex technological and organizational systems* [16].

Formulation of the events, decisions, and causes of accidents such as *Exxon Valdez* lead to further understanding of how to manage controllable errors in operations of marine systems. Engineers, managers, regulators, and operators must be made aware of their role in reducing human and organizational errors. Qualitative and quantitative HOE analyses should compliment each other: qualitative analysis should form a basis for quantitative analysis. Only through making explicit considerations for human errors in reliability based analyses, can we reduce the likelihood of similar accidents like *Exxon Valdez*.

Acknowledgments

The author would like to recognize the insights, guidance, and leadership in this work provided by Professor Robert Bea of the Departments of Naval Architecture & Offshore Engineering and Civil Engineering at the University of California at Berkeley, and Professor Karlene Roberts of the Haas School of Business Administration at the University of California at Berkeley. Key items of data and information for this work has been provided by the Marine Investigation Group of the National Transportation Safety Board.

This work is a result of research sponsored in part by NOAA, National Sea Grant College Program, Department of Commerce, under grant number NA89AA-D-SG138, project number R/OE-17, through the California Sea Grant College, and in part by the California State Resources Agency. The U.S. Government is authorized to reproduce and distribute for governmental purposes.

This work also has been sponsored in part by Chevron Research & Technology Company and Chevron Shipping Company, Amoco Production Company and Amoco Transport Company, Unocal Corporation, the California State Lands Commission, the U.S. Coast Guard, the U.S. Minerals Management Service, and the American Bureau of Shipping. The support and guidance of these sponsors is gratefully acknowledged.

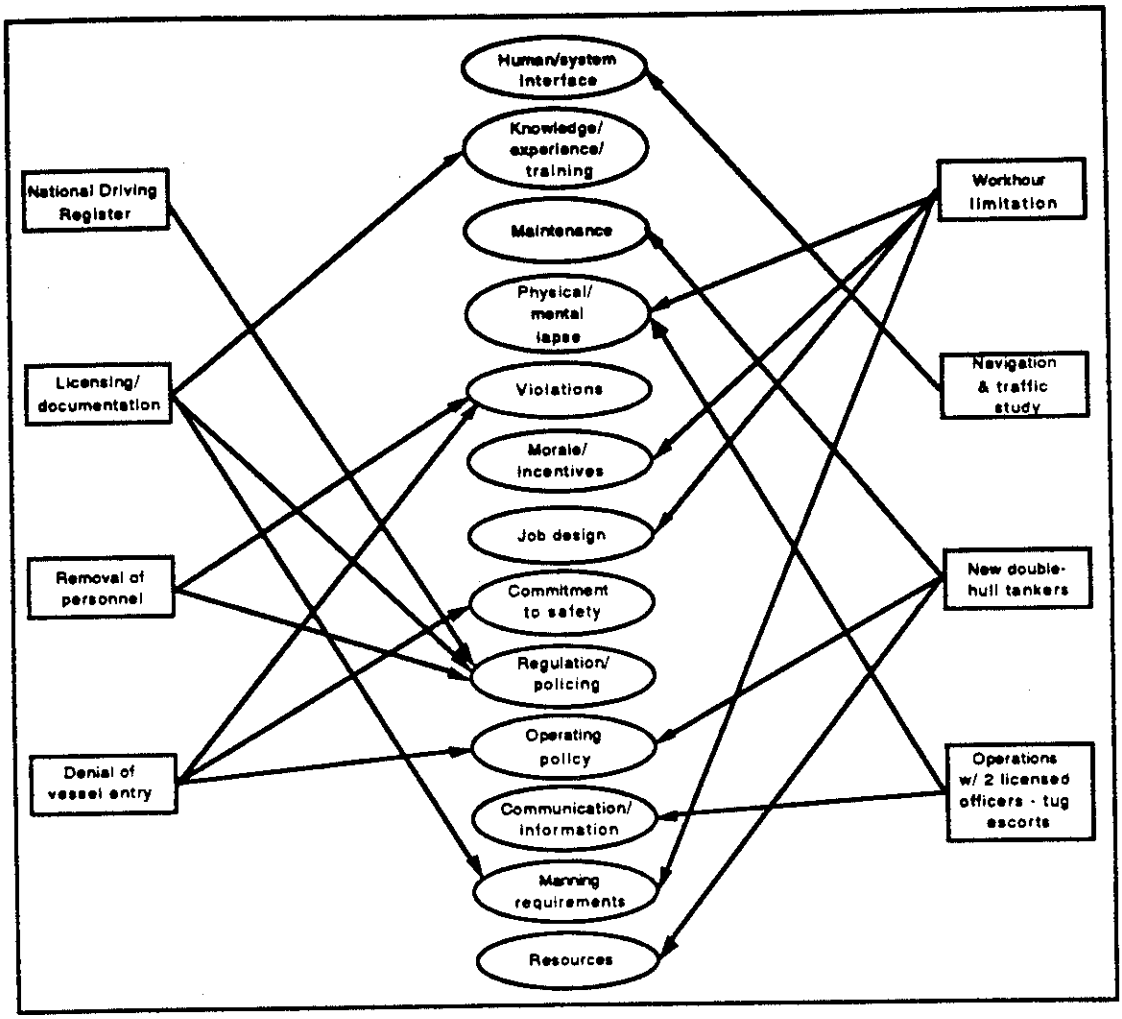


Figure 5: Influences of Oil Pollution Act of 1990 on HOE related accident causes

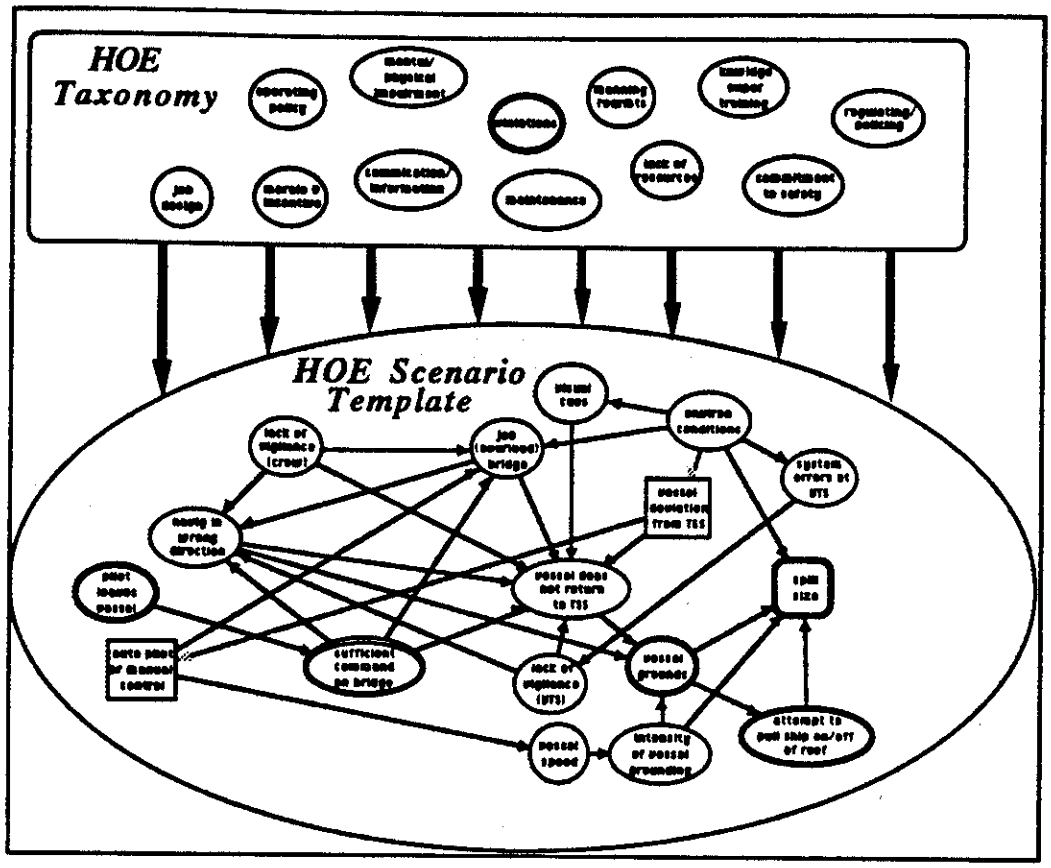


Figure 6: Influence diagram template for vessel groundings

References

[1] Paté-Cornell, M.E. & Bea, R.G. (1989) "Organizational aspects of reliability management: Design, construction, and operation of offshore platforms," Research Report No. 89-1, Department of Industrial Engineering and Engineering Management, Stanford University.

[2] Marton, T. & Purtell, T.W. (1989) *Investigations In The Role Of Human Factors in Man Related Marine Casualties.* U.S.Coast Guard Internal Report.

[3] Wenk, E., Jr. (1986) *Tradeoffs, imperatives of choice in a high-tech World.* Baltimore: The Johns Hopkins University Press.

[4] Bea, R.G. & Moore, W.H. (1991) "Management of Human and Organizational Error in Operational Reliability of Marine Structures", *Proceedings, Society of Naval Architects and Marine Engineers 2nd Offshore Symposium: Designs and Codes.* Houston, TX.

[5] Reason, J. (1990) *Human Error.* Cambridge University Press: New York.

[6] Davidson, A. (1990) *In the Wake of the Exxon Valdez.* San Francisco: Sierra Club.

[7] Brady, E.M. (1960) *Marine Salvage Operations.* Centreville, MD: Cornell Maritime Press.

[8] Roberts, K.H. & Moore, W.H. (1992) "The Gordian Knot: Into Which Sailed the *Exxon Valdez*". Research Report No. 92-1, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering, University of California, Berkeley.*

[9] National Transportation Safety Board. (1990) *Grounding of the U.S. Tankship Exxon Valdez on Bligh Reef Prince William Sound near Valdez, Alaska.* PB90-916405, NTSB/MAR90/04.

[10] National Research Council. (1990) *Crew Size and Maritime Safety.* Washington, D.C.: National Academy Press.

[11] Government Accounting Office. (1988) *Report to the Chairman, Subcommittee on Coast Guard and Navigation, Committee on Merchant Marine and Fisheries, House of Representatives* (November) (GAO/RECD-89-48).

[12] Keeble, J. (1991) *Out of the Channel: The Exxon Valdez Oil Spill in Prince William Sound.* New York: HarperCollins Publishers.

[13] National Transportation Research Board. (1990) *Exxon Valdez Casualty Factual Reports.*

[14] Phillips, L.D., Humphreys, D.E. & Selby, D.L. (1990) A socio-technical approach to assessing human reliability. From *Influence diagrams, belief nets and decision analysis.* (Chapter 13) Edited by Oliver, M.R. & Smith, J.Q. Wiley & Sons: New York.

[15] Connaughton, S.T. (1990) Vessel pollution prevention and response considerations. *New Oil Pollution Act of 1990 Conference.* Government Institutes, Inc.

[16] Bea, R.G. & Moore, W.H. (In prep.) "Improving Operational Reliability of Marine Systems: Management of Human and Organizational Errors". *New Challenges to Organizations, High Reliability Organizations*, McMillan: New York.

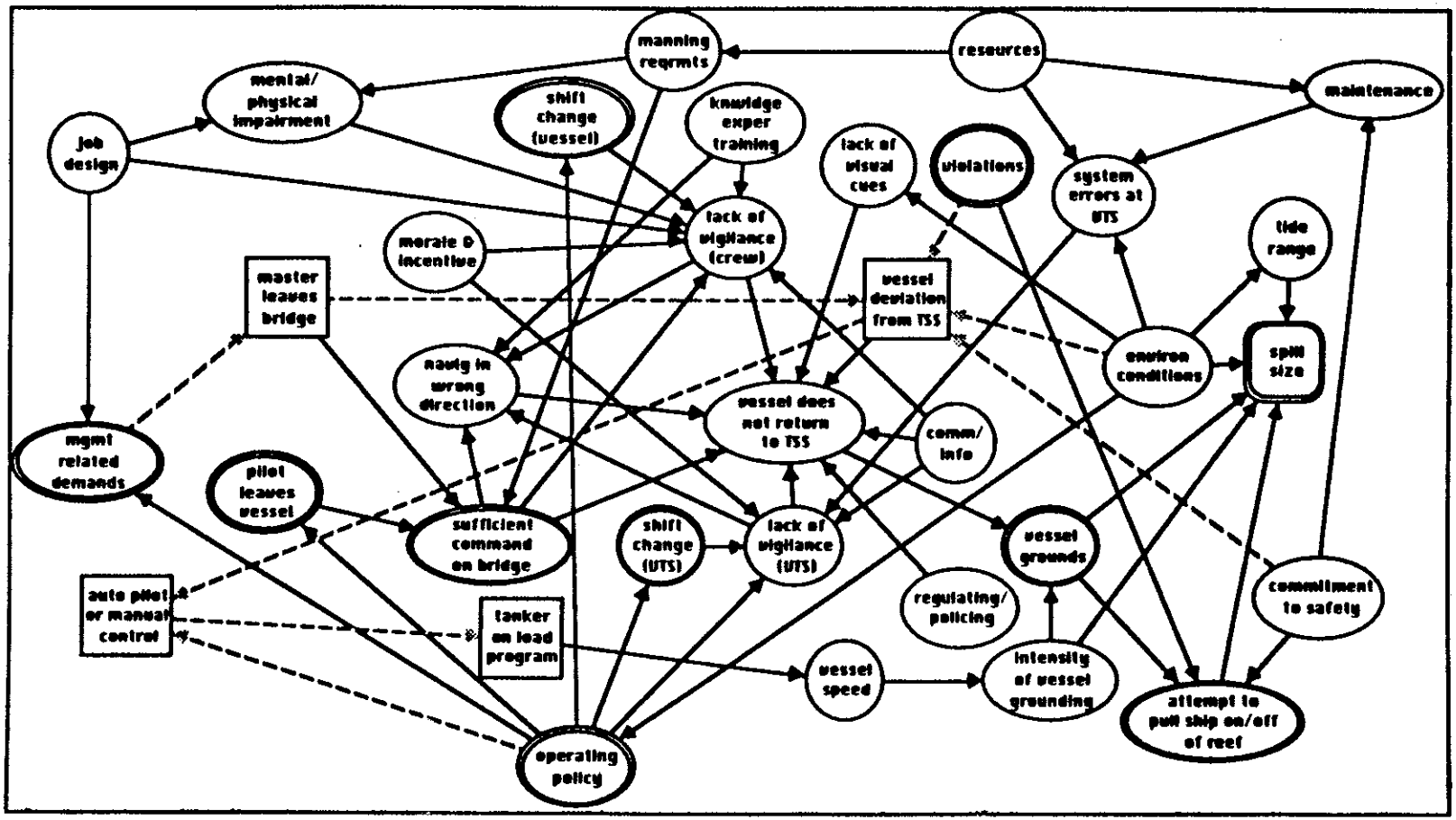


Figure 3: Influence diagram representation of factors leading to grounding of *Exxon Valdez*

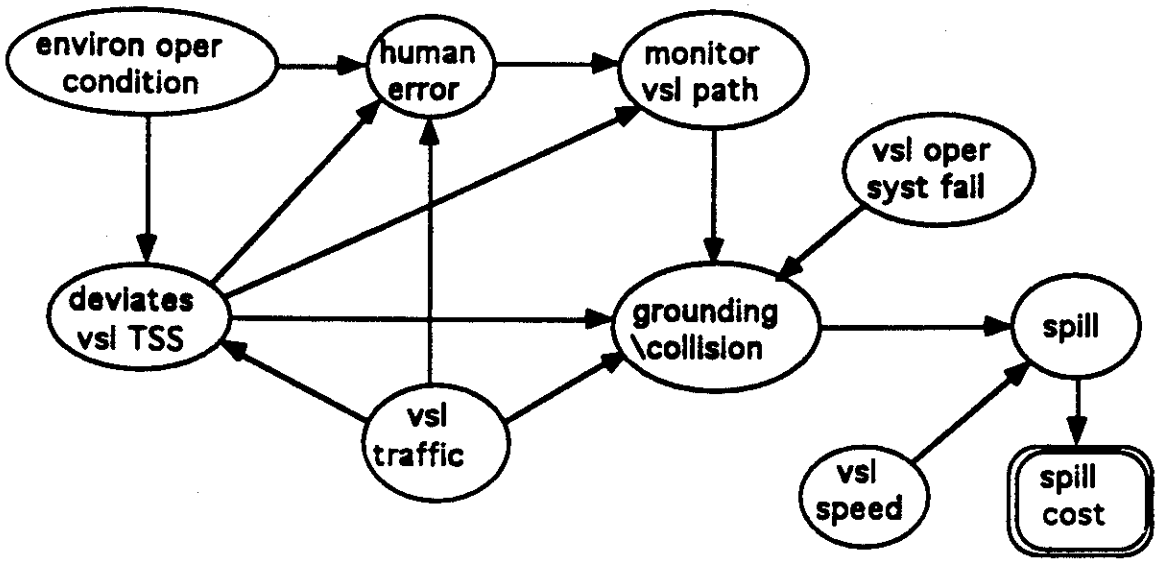


Figure 4: Influence diagram model of major factors involved in tanker grounding or collision

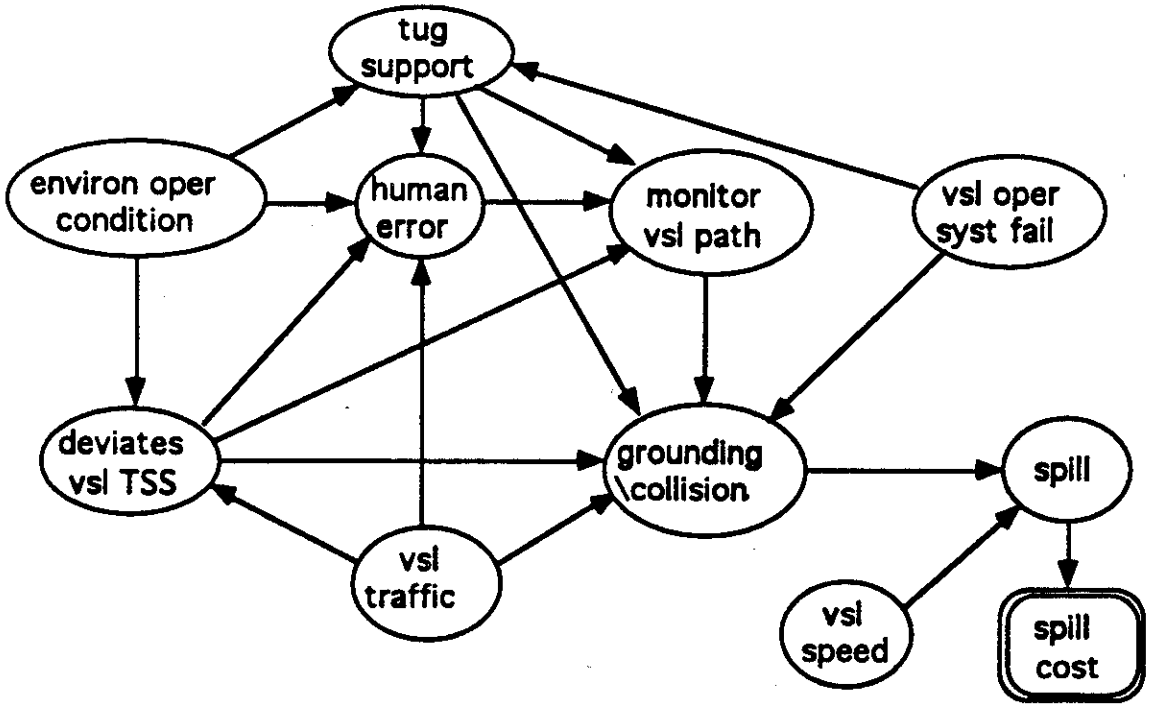


Figure 5: Influence diagram to model the effects of tug support

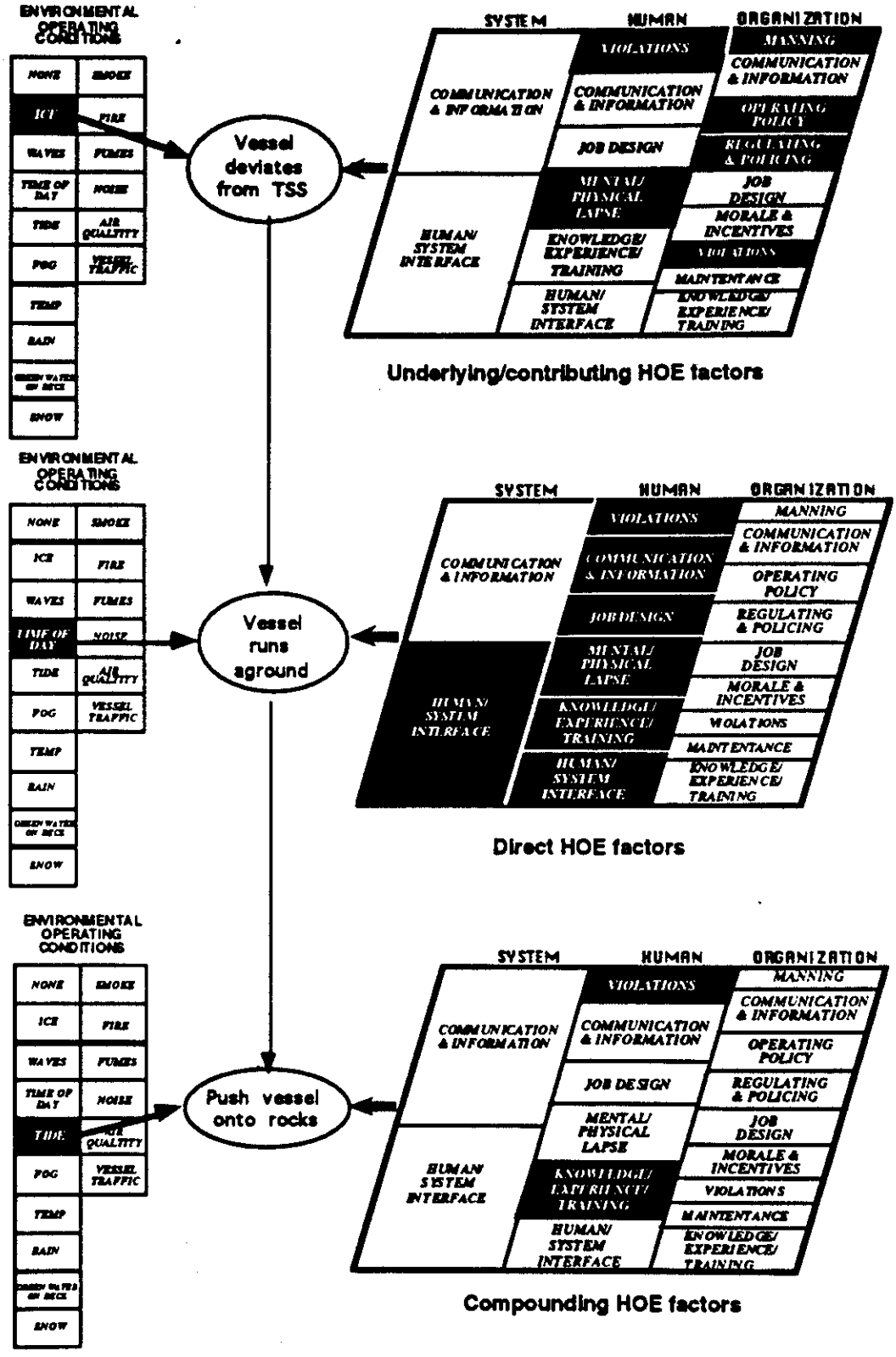


Figure 1: HOE influences on the events involved in the grounding of *Exxon Valdez*

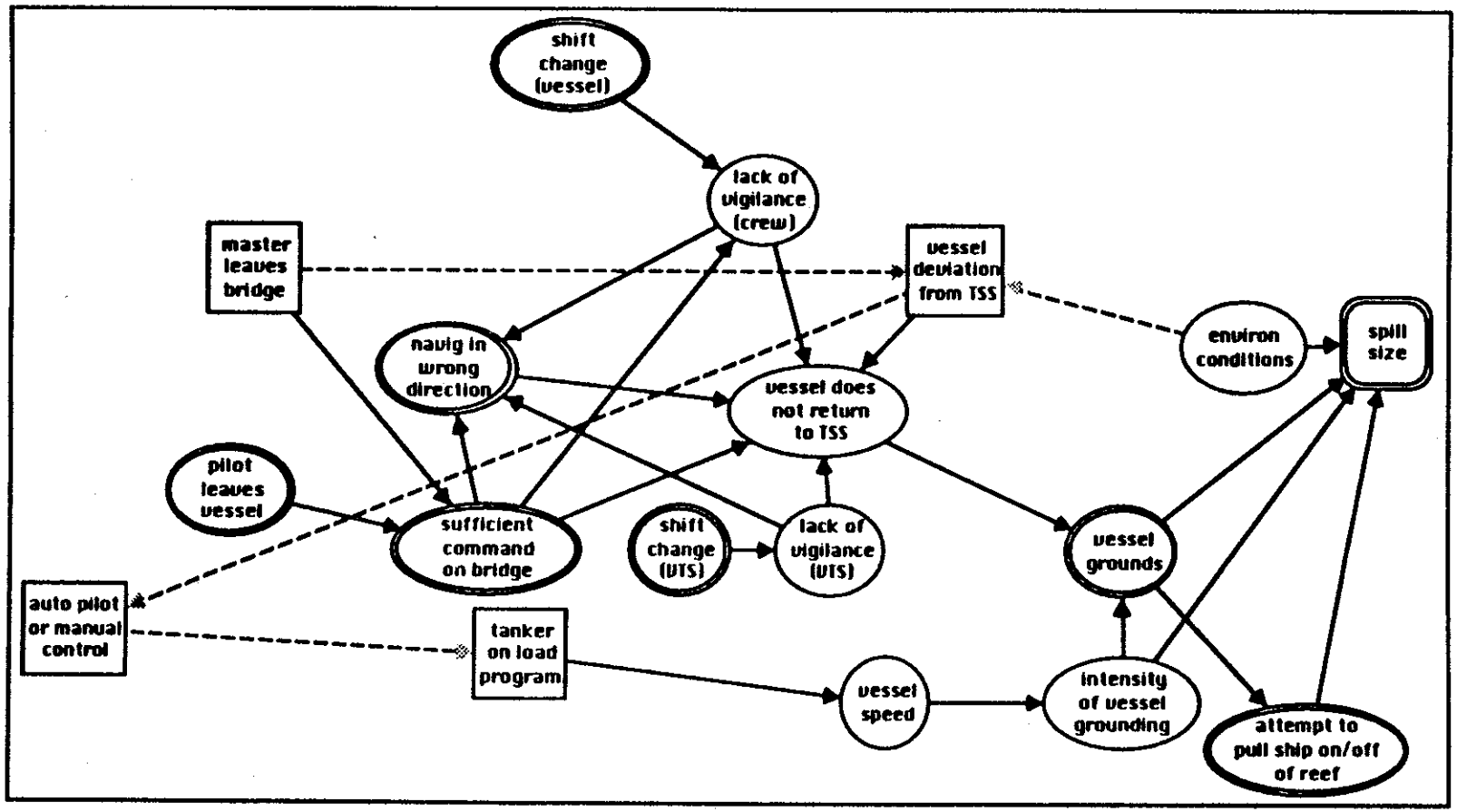


Figure 2: Influence of events and decisions leading to grounding of *Exxon Valdez*

Risk Analysis, Vol. 12, No. 1, 1992

Management Errors and System Reliability: A Probabilistic Approach and Application to Offshore Platforms

M. Elisabeth Paté-Cornell[1] and Robert G. Bea[2]

Received October 17, 1989; revised June 18, 1991

Probabilistic risk analysis, based on the identification of failure modes, points to technical malfunctions and operator errors that can be direct causes of system failure. Yet component failures and operator errors are often rooted in management decisions and organizational factors. Extending the analysis to identify these factors allows more effective risk management strategies. It also permits a more realistic assessment of the overall failure probability. An implicit assumption that is often made in PRA is that, on the whole, the system has been designed according to specified norms and constructed as designed. Such an analysis tends to overemphasize scenarios in which the system fails because it is subjected to a much higher load than those for which it was designed. In this article, we find that, for the case of jacket-type offshore platforms, this class of scenarios contributes only about 5% of the failure probability. We link the PRA inputs to decisions and errors during the three phases of design, construction, and operation of platforms, and we assess the contribution of different types of error scenarios to the overall probability of platform failure. We compute the benefits of improving the design review, and we find that, given the costs involved, improving the review process is a more efficient way to increase system safety than reinforcing the structure.

KEY WORDS: PRA; organization; management; probability; offshore platforms.

1. INTRODUCTION

Many failures of engineering systems are caused by human errors (see, e.g., Ref.1). Some of these errors, such as the failure of an operator to perform a particular task, are included in Probabilistic Risk Analysis (PRA).[2] Their probabilities are estimated on the basis of diverse databases, laboratory experiments, and expert opinions. The analysis, however, is generally based on the assumption that the system conforms to expectations—that is, that there is no major flaw in the design, that construction was done according to the plans, and that the procedures of operation are generally adequate, even though an operator may fail to perform a specific task. Most of the uncertainties, in such an analysis, thus, reflect a residual randomness in loadings, components, or operator performance, seldom the possibility that, in reality, the system is not what engineers and managers believe it to be. Thus, PRA accounts for the possibility of accidents triggered by identifiable initiating events (including operator errors) and, in particular, by high levels of loads that exceed the design capacity. If the choice of the design criteria was reasonable, this last case can legitimately be considered as "bad luck."

As it is shown here for jacket-type offshore platforms, this kind of "bad luck" may contribute only a small part of the probability of failure. A large fraction

[1] Department of Industrial Engineering and Engineering Management, Stanford University, Stanford, California 94305.
[2] Department of Civil Engineering and Department of Naval Architecture and Offshore Engineering, University of California, Berkeley, California 94720.

0272-4332/92/0300-0001$06.50/1

of it may be attributable to errors and bad decisions rooted in the organization itself, which affect the PRA inputs but are not accounted for explicitly (even though their effects may appear implicitly in performance statistics and expert opinions). These bad decisions may involve errors of reasoning, excessive risk-taking, or unwarranted optimism. In some instances, however, they may reflect rational choices given the procedures as set and they do not enter clearly the classic "human error" framework. For example, the organization may not be equipped to observe particular types of warning signals, to perform under time pressure, or to learn from near-misses.[3] Organizational errors thus encompass some (but not all) of the classical human errors and other factors, such as communications and incentive problems, that may contribute significantly to the probability of system failure.[4,5]

The link between management and system reliability has received some attention in recent engineering studies,[6–8] with particular interest for the effect of design and construction errors on the structural reliability of systems subjected to seismic loads.[9,10] Specialists of organizational behavior have studied management characteristics that influence system performance and seem to lead to "high-reliability" operations.[11,12] Others have pointed out the role of management errors in past system failures, and concluded that an engineering-based PRA is a futile exercise to the extent that it does not encompass these possibilities,[13] or that social scientists may know something that the engineers don't in their assessment of the actual risk.[14] This is not necessarily the case to the extent that the effects of management errors are implicit in the database. PRA is a logical starting point because, for a system to fail, one of its failure modes has to occur regardless of the root of element failures. If the subsystem that is weakened by an organizational error is critical, the system is directly threatened and the problem requires immediate attention as the component failure may cause a disaster. The accident of the Piper Alpha offshore platform is an example of critical subsystem failure rooted in several organizational problems, including failure of communications and failure to take corrective action given early warning signals of an impending catastrophe (see, Ref. 15).

PRA is designed to provide information about subsystem criticality and failure-mode probabilities and can be used, before an accident occurs, to set priorities among different types of measures aimed at improving reliability under resource constraints. These measures can be purely technical (e.g., add a redundancy in one of the subsystems) or they can be organizational (e.g., provide incentives to seek further information when needed). The objective of this paper is to assess the effects of some organizational and economic factors on system reliability. PRA is used as a calibration tool to obtain a coarse assessment of safety gains from a variety of organizational modifications. The approach is to start from the system and its failure modes, to identify the decisions and potential errors that affect the inputs, and to relate these to features of the organization. As an illustration, the effect of management errors for jacket-type offshore platforms (see Fig. 1) is analyzed for the three major phases of their lifetime: design, construction, and operation. The proposed model accounts for the possible accumulation of several errors over the structure's lifetime, with synergistic effects on the system's capacity.

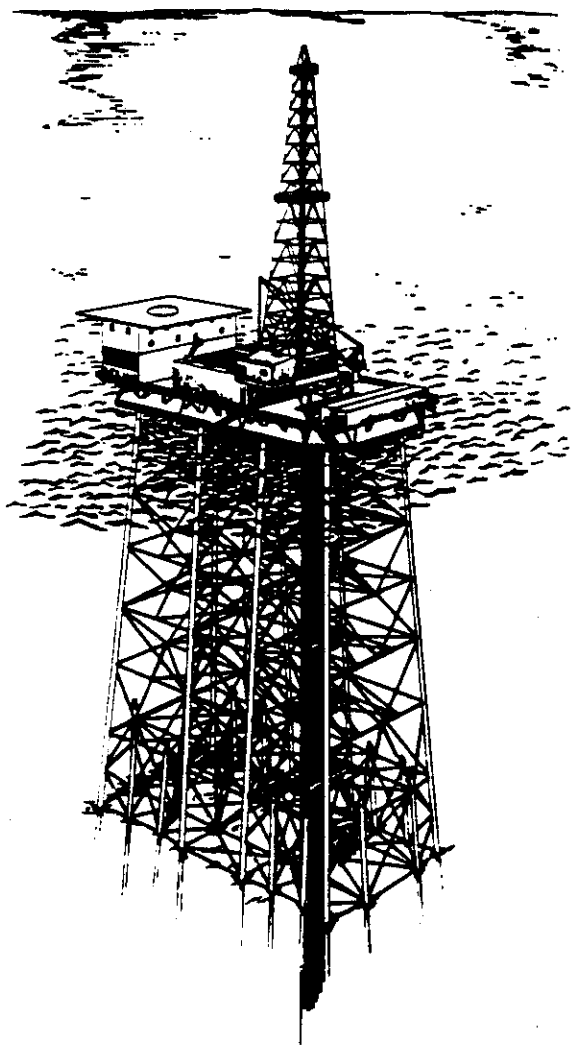


Fig. 1. Example of jacket-type offshore platform.

2. ORGANIZATIONAL ASPECTS OF RELIABILITY MANAGEMENT

2.1. Organizational Features and Organizational Errors

Collective decisions result from sequences or conjunctions of individual decisions. Generally, two classes of problems face an organization in situations of distributed decision-making: information problems (who knows what and when), and incentive problems (how are individuals rewarded, what is their margin of maneuver, what decision criteria do they use, how do these criteria fit the overall objectives of the organization?).[16–21] Key organizational elements of system reliability are thus: *individual skills, information* (collection, communication, and learning), *resource constraints* (e.g., schedule and budget set by corporate goals), and the *reward system* (job appraisal, wage increases, cost to the employee of delays and mistakes, incentives, etc.), particularly as it affects the balancing of objectives such as costs and safety. These factors, in turn, are rooted in the structure, the procedures, and the culture of an organization,[8,22] all of which therefore contribute to the safety of its product or operation. Several taxonomies of human errors have been proposed, often to understand the psychological roots of human actions such as intention[23] and to classify data about human errors. Rasmussen[24] proposes a taxonomy of human malfunctions based on an analysis of an operator's mental activity. Reason (ibid.) bases his "generic error-modelling system" on the distinction among skill-based, rule-based, and knowledge-based behaviors and considers different levels of rationality. Norman[25] bases his analysis on the difference between slips and mistakes (intentional). Rouse[26] focuses on diagnosis and correction of systems' malfunctions. More recently, Reason[27] proposed a framework for a theory of "human contribution to organizational accidents" based on a key distinction between "types" (managerial factors) and "tokens" (individual actions).

Our taxonomy of operators' errors allows us to relate individual decisions to organizational features such as information and reward systems. In risk situations, where uncertainty is a key element and risk attitudes are determinant factors, our fundamental distinction is between gross errors (in unambiguous situations) and errors of judgment (under uncertainty) (see Fig. 2). This distinction becomes fuzzy in situations of uncertainty where there is an agreement on a proper course of action. In general, however, gross errors reflect mostly information problems, whereas errors of judgment involve issues of incentives, preferences, and rationality.

2.2. Gross Errors

Gross errors are caused by a temporary or permanent lack of knowledge, misunderstanding of a situation, or someone's inability to respond to specific circumstances. We divide them further among communication problems, cognitive problems, and problems due to human limitations.[28,29] Communication failures can occur because the necessary information is not gathered in the first place, communication channels do not exist, or the existing channels do not function. These malfunctions can be caused by unreliable procedures, failure of communication equipment, lack of informal communications, or deliberate retention of information. This last case (tendency to secrecy) may be rooted in the culture of the corporation or in an incentive system that causes internal conflicts and unwillingness to share information and power.[30] Communication problems also include distortion of information as in the classic game of telephone, either unwillingly or because information is systematically biased toward optimism and bad news is filtered out.

Cognitive problems can involve accidental slips, use of the wrong models, and genuine ignorance.[25,31] In the first case, an employee, although he has *a priori* all the required knowledge, makes an error due to a variety of causes such as overload, stress, or boredom, some of which can be traced to job design; or because he is overwhelmed by the system's complexity.[32] In the second case, the employee may believe firmly in a wrong model, for example, because he makes a mistake in transposing experience from another field,[33] or because he makes an error of logic in interpreting incomplete information and, for instance, jumps to conclusions that limited evidence does not support.[34] In a third case, he may be aware of his ignorance but decides to pick one available solution because he cannot, or does not, want to acquire additional information. In this last case, not only the information or the fundamental knowledge are not available, but the incentive system fails to motivate the decision-maker to seek additional information.

Gross errors (as well as errors of judgment) can also be caused by human physical and psychological limitations. The basic cause can be a combination of severe circumstances and physiological incapacity to deal with an unusual environment (e.g., on an offshore platform, sea sickness, vertigo, inability to see in the dark, or sheer exhaustion). Mental limitations leading to gross errors

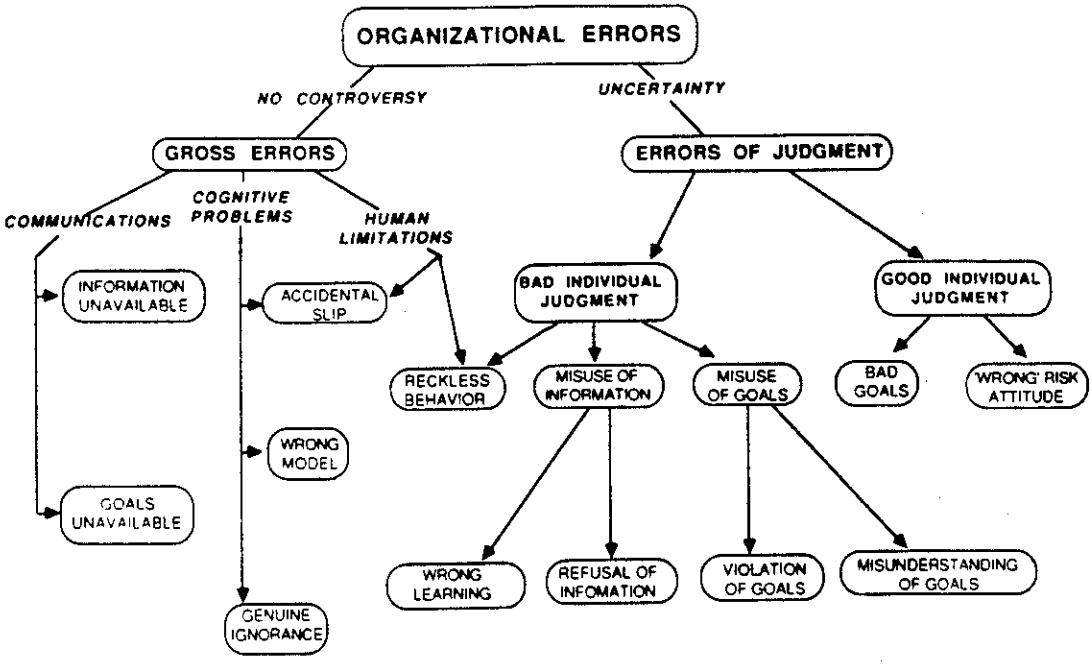


Fig. 2. A taxonomy of organizational errors.

include panic, laziness, or sheer stupidity. The root of these problems may be in procedures of selection and training of the personnel that result in a mismatch between performance expectations and the general working conditions (e.g., the work schedule), or between the job demands and the capabilities of specific individuals.[35]

2.3. Errors of Judgment

Errors of judgment are those that occur under uncertainty and are open to interpretation for two categories of reason: incomplete information and diversity of risk attitudes and preferences. Contrary to gross errors, they cannot be easily defined by a violation of a deterministic truth. Our approach is based on a loose assumption of "bounded rationality."[36] Clearly, under some circumstances, operators can shift to a totally different, irrational mode ("I don't know and I don't care"). This shift can be triggered by panic, anger, or other incapacitation and can lead to disasters.[24] Yet people generally respond to the reward system and use, to some extent, available information—even when incomplete. Interpretation of imperfect information requires a subjective element even though, to be properly done, it must follow a certain logic. Violation of this logic is one key source of errors of judgment.[34] Furthermore, risk attitudes and valuation of trade-offs obviously vary, and there can be a mismatch between individuals and the organization. The questions are thus: What constitutes "good" or "bad" corporate judgment? And how can one achieve compatibility between individual risk attitudes between individuals and the interests of the organization?

"Bad" corporate judgment is generally closely linked, in the corporation's own assessment, to outcomes of past decisions that have been judged unsuccessful by criteria that are both ambiguous and variable[37] and therefore of little value *ex ante*. In any case, corporate judgment can be seriously questioned when the corporation simply violates the laws and the traditions of the profession or society at large, or when it simply ignores risks because it is not equipped to observe hazard signals, or willing to recognize, communicate, and process uncertainties. Furthermore, the organization may neglect or suppress dissonant information and engage in "group think,"[38] leading to risky decisions. If this is not the case, and if the value system of the corporation is socially and internally acceptable, the corresponding risk attitude can be used as point of reference as to what constitutes "good judgment." The objective is then to design an incentive structure and feedback mechanisms that ensure compatibility between individual preferences and the interests of the corporation.

Even if one adopts this definition, an error of judg-

ment when it occurs may not be unanimously considered as such. First, interpretation of evidence given incomplete information may vary among individuals.[39] Second, there generally remains in a group a spectrum of individual preferences that vary with aspirations.[40] Third, corporate attitude toward risk may appear ambiguous and variable and may induce what appears for the observer a still-wider spectrum of risk attitudes. Under severe time or budget constraints, individuals may take risks that they would naturally avoid if the incentive system provided them with alternatives.[41,42] More generally, risk-taking is the prevalent attitude when the prospects involve losses, whereas risk aversion dominates the decisions of individuals facing prospective gains,[43] and corporations are seldom equipped to compensate for the aggregate effect of individual decisions on corporate decisions.[44] On the other hand, the same aggregate effects may make individual risk-taking acceptable to a more conservative organization.[45] Yet what is perfectly rational at the individual level may in fact constitute an error of judgment from the corporate viewpoint, when the management does not realize the implications of the goals and incentives that it sets. Our analysis of errors of judgment thus relies on a critical distinction: bad judgment at the individual level, either in interpretation of information or in preferences, and good individual judgment (given the constraints imposed on the employee and his own value system) lead to decisions in contradiction with the interests of the corporation.

We further divide bad judgment at the individual level among reckless behavior, refusal to believe or to use available information about uncertain quantities—for example, because it does not seem to fit the organization's objectives[46]—misunderstanding of goals or violation of the organization's rules, and wrong learning mechanisms. Learning from incomplete information (e.g., a very small sample of relevant facts) involves gradual updating given new pieces of evidence, but many known biases can occur in practice in this exercise.[34] When this updating is properly done, however, the logical treatment of prior probabilities, base rates, and partial failures can provide valuable information.[47]

Rational individual decisions that appear as an error of judgment from the corporate viewpoint may be the most interesting case; for example, the aggregate effects of individual risk-taking when facing losses and risk aversion when facing gains. They raise questions of incentive compatibility and call for rewards and feedback mechanisms that often do not exist (see, e.g., Ref. 42 on principal-agent problems). Central to the management of critical systems are trade-offs, such as production vs. safety. Production goals handed down without indication of how these trade-offs should be treated can give the operators greater latitude and responsibility, and sometimes enhance system safety. They can also be a primary source of errors of judgment if there is no solution that would actually be acceptable to management under the constraints that they have set, if the preferences of the agent do not match that of the organization, or if he is not capable of handling the situation.[35] Furthermore, these errors are bound to repeat themselves unless the organization recognizes the problem and decides to change the rules.

3. EXAMPLES OF ORGANIZATIONAL FAILURES IN THE U.S. OFFSHORE INDUSTRY

The following case histories have been chosen as illustrations of some of the organizational errors described above. They involve technical failures that could at first be attributed to "human errors" but are rooted deeper in the organization. These failures are similar to those observed and described by Carson[41] and Stinchcombe and Heimer.[48]

3.1. The Platform That Slid

In 1966, an offshore lease was purchased. The site surveys showed an unusual bathymetry and an initial evaluation indicated the potential for mudslides. A study was initiated in 1967 to investigate this phenomenon and evaluate the risk. The design of a conventional platform was commissioned (1967) on the premise that if the risk of mudslide was found to be too high, the platform would be sited elsewhere and a mudslide-resistant platform would be designed for the location. The design was completed before the risk study. The management made the decision to start the construction of the platform so that, if the study indicated that the site was safe, the project would be on schedule. When it was completed, the risk study confirmed the presence of mudslides and indicated that the risk of failure at the proposed site was 10–100 times greater than for a conventional site. The recommendation was made not to site a conventional platform at the proposed location. The management and the technical team met to discuss these recommendations. A technical report was written stating that, if a conventional platform was installed at the site, it would fail in a short period of time due to overloading by mudslide forces.

The management, however, made the decision to site the conventional platform at the proposed location:

by then, there was so much pressure to pursue this project that management decided to take the risk of a mudslide that they still estimated less likely to occur than not. The lead engineer refused to sign the final construction drawings. One platform failed and an adjacent platform moved downslope during a storm in August 1969. The sliding was discovered when workers tried to run tools through the well conductors. Laser surgery of the piles disclosed significant platform movement. The still-standing platform was then declared a constructive loss and an insurance claim was made. Both platforms, however, were salvaged. The managers involved in the decision suffered career by-pass and eventually left the company. These managers stated that they never believed in the slide hazard. The technical staff involved suffered the opposite type of credibility crisis: management after this episode started believing them too much without asking questions.[49]

The sequence of errors described above came from a commitment without proper information. When this information became available, the time pressures were such that the management had strong incentives to dismiss it. By then, it had lost a lot of its value due to poor timing. The result is a cumulation of errors of judgment that can be described as the combination of: (1) an imprudent decision to begin the work without the test results when prior information indicated that the soil condition seemed problematic; and (2) a refusal to use the information when it became available because it revealed that the previous move was a mistake (an "escalation of commitment," similar to those described in Ref. 50).

3.2. The Mobile Drilling Rig That Could Not Find a Proper Site

During the winter of 1979, a mobile drilling unit, originally designed for the storm conditions of the Gulf of Mexico, was proposed for siting in Lower Cook Inlet, Alaska. The platform, located offshore of California, was preparing for transfer to Alaska. The client oil company contracted a consultant to make a risk assessment for siting the platform in Alaska. Data were gathered on site conditions as well as the conditions of the unit, looking for fatigue damage to the legs from long tows. A risk assessment was made and the results were compared to risks of failure during the storm season if the same unit were sited in the Gulf of Mexico. They indicated that the risk in Alaska was 10 times greater at that time of year than in the Gulf of Mexico, where the overall annual probability of failure was estimated at 0.02. In Alaska, the probability of failure was assessed at 0.2 per year during the winter months (i.e., 0.05 for a 3-month period of severe winter conditions). The consultants recommended explicitly not to site the units during the proposed period but, rather, 2 or 3 months later when the chances of storms and icing were lower and the failure probability was estimated to be back to the same level as in the Gulf. The client oil company did not want to wait because of the costs involved ($100,000 per day) in putting the unit on standby for 2 or 3 months. Note that the rationality of this decision can be challenged simply on the basis of expected costs. Given that the cost of failure of this type of platform is on the order of $1 billion, the expected value of the failure costs for 3 months of Alaska winter is on the order of $50 million ($0.2 \times 0.25 \times 10^9$), whereas the cost of 90 days of delay is $9 million.

The client decided to discuss the risk of siting with the rig owner, the rig operator, the rig classifier, the rig mover, and the rig insurer. The risk assessment was presented to this decision-making group and a report was written summarizing the results. The group decided that the risk was too great to site the rig during the initially proposed period, and the decision was made to delay the siting until after the winter storm season. The group asked the consultant if they really believed their risk assessment results, which the consultant confirmed. The client required the presence of the consultant onboard during the starting of operations, as one's perspective on risk may change as a function of one's proximity to it. The unit operated without incident and was later taken to Norton Sound, Alaska. The risk assessment was then repeated, this time with respect to scour (erosion of the sea floor by currents) around the rig's footing. The results indicated that the probability of scour was high; but the operator company decided to delay scour protection work until the problem actually occurred—the rationale being that it could be remedied at that time. The unit was placed in Norton Sound. Footing scour did occur and protection had to be placed in order to prevent damage to the rig. Two divers were killed during the placement of the scour protection. The unit ran out of work in Alaska and was then towed from Norton Sound to California. During the transit, a mysterious flooding occurred: a door was left open and, to this day, no one understands how it happened. The unit sank in the Aleutian trench in 6000 ft of water. The rig owners collected the insurance. The loss was therefore encurred by the insurance company.

Here again, the fundamental problem is an error of judgment on the part of management: the failure to consider in time a particular type of external event (scour)

that later threatened to cause platform failure. It is an information error that was probably induced by earlier difficulties and costs due to delays in the relocation of the structure. It seems that the decision-makers, having already encurred the costs of the prudent decision to delay the Alaska siting, did not want to hear more about potential problems (a classical sunk cost recognition problem). The final error can be traced to a refusal of information and a breakdown in communications.

3.3. The Platform That Embedded Upside Down

A platform steel jacket was designed to be launched like a ship from a floating barge and towed to the platform site. The jacket weight and buoyancy were checked to determine if the jacket would float after launching. The calculations indicated that additional buoyancy tanks were needed to make the jacket float. Buoyancy tanks were added and placed at the upper face of the top end of the jacket. The jacket was launched from the barge, but because of very high momentum when the jacket rotated, the buoyancy tanks at the upper face of the top end were ineffective at slowing the jacket's movement. The jacket embedded upside down. The buoyancy was then insufficient to raise the top of the jacket that had more stability upside down. The closure plates of the legs leaked due to bad welds and the reserve buoyancy was lost. Due to bad weather, it took 2 months to right the jacket. At a cost of $150,000 per day, the total cost was $9 million. The next engineer who designed a similar structure decided to launch it in deep water 15 miles from the intended location then to tow it to the site. During the tow, the jacket swang against the towing barge and crushed two legs. The jacket had to be towed into shallow waters to expose the legs. The damaged portions of the legs had to be cut out and new sections were welded in. At $150,000 per day, the cost of this 3 months delay was $13.5 million. In trying to avoid the first error, a second error had been committed that added to the costs of the first one. This story was kept confidential until it occurred again 2 years later, this time in the Santa Barbara channel. At that point it was circulated in the industry and later included in some university-level courses on marine structures.

The case of the jacket that embedded upside down can be traced to a gross error due to lack of experience. Although some checking did occur and an initial defect was revealed, the corrective action that followed was insufficient to fix the problem. The second error was a repeat of the same phenomenon. Both errors were cases of wrong understanding (i.e., wrong models) of the dynamic behavior of the structure during the launch and during the tow. Whereas the problem was well known in the industry, inexperienced engineers committed the same error one after the other: the lesson, when it was learnt the first time, was not communicated to the rest of the industry.

3.4. The Platform Without a Foundation

At the site of a proposed platform, consultant A took soil borings and found unusual soil conditions. Foundation pile load tests were performed and they confirmed the unusually brittle nature of the soil at the site. The design of a platform was initiated for a new location several miles from the emplacement of the soil borings and the pile tests. For the new location, the company bid soil borings. Consultant A was not the low bidder. The job was awarded to consultant B who then performed the boring and found the same unusual (brittle) soil. *In situ* tests (by cone penetrometers) were used to determine the soil strengths. Samples sent to a laboratory for additional testing confirmed the strengths measured by field tests. The results of the field and lab tests were sent to engineering and an analysis of the foundation was performed. This analysis presumed "ductile" (elastoplastic) soil stress-strain characteristics. Soil strengths based on *in situ* and lab test results showed that, in reality, the soil seemed to be very brittle. This implied that the capacity of the foundation piles had been dramatically overestimated. Because of the highly competitive environment in which consultants operate, the pile load tests that had been performed by consultant A were ignored. Those tests confirmed the unusual nature of the soil behavior. The first design of the foundation was based on drilled and grouted piles. When the platform bids were received, very high costs were attributed to drilling and grouting. A contractor proposed to drive piles and save money. This low bid option was chosen. The contractors expected pile-driving problems and a large number of hammer blows to drive the piles. In addition very large hammers were required to do the job.

Actually, many piles did not have to be driven to reach the design penetrations: they sank under their own weight. The hammer was used to drive the piles a few feet into stronger soils. Due to gas supply contract pressures, the decision was then made to proceed with the installation of the platform and the facilities. The platform was installed and placed in operation. The company engineers then decided to perform a pull-out test on a well conductor. They found that the conductor capacity was equal to the weight of the conductor itself

and that there was no skin or shaft resistance. Until the foundation was fixed, the platform therefore had to be "de-rated." This required that the personnel be evacuated and the wells shut-in in advance of storms that occur several times every year. Other observations and tests were made on the platform and on the soil around it. They confirmed the foundation problem. A massive study was undertaken to find a remedy. It took five years and $500 million to fix the problem. The platform was then given a "100 year" certificate of insurance. The low price bid obviously did not lead to the least costly solution in the long run.

This case is more complicated and involves a combination of errors. A gross error was made at the beginning of the job by the contractor who came up with the lowest bid and by those who accepted it. There was then an error of judgment at the time of field installation when the contractor observed that something was going wrong and that the procedure might be inappropriate but proceeded with the plan without seeking appropriate information.

4. JACKET-TYPE PLATFORMS' RELIABILITY AND EFFECT OF ERRORS

Risk and uncertainties are unavoidable in the management of critical facilities in general, and of offshore platforms in particular; but errors in decisions about such risks are often avoidable. The error analysis that follows is based on our fundamental distinction between gross errors and errors of judgment. (This distinction is ours and not one that is customary in industry.) Errors of both types are further divided among three severity levels—high severity, low severity, and no error—in order to characterize their effects on the system.

Our general approach relies on a PRA model and on an analysis of the different phases of the industrial process (such as design, construction, or operation). Each *input of the PRA* model can be related to *decisions or actions* within the process. These decisions and actions are characterized by the *actor* (decision-maker or operator), the procedures, the information, the rewards structure, and the resource constraints, which in turn can be linked to the relevant *organizational factors*.

Consider as an illustration the case of the two possible designs of jacket-type offshore platform: an X-design where each of the members has some redundancy (it takes a sequence of any two failures to cause jacket failure), and a K-design where the braces numbered 2 and 3 do not have a backup (see Appendix A). Assume for simplicity that these two structures can only be subjected to two types of loads that constitute the *initiating events* of the failure: wave loads and boat collision. The occurrences of wave loads are not affected by human actions, whereas boat collisions involve several decisions, such as reaching the platform given the weather, and the choice of a maneuver. Furthermore, wave loads and boat collision are correlated. Appendix A presents an example of the model structure described above, from PRA to technical failure causes, to decisions and human errors, to the organizational roots of these errors.

The analysis of the whole platform is done here at a high level of aggregation (i.e., considering only the three main subsystems: foundation, jacket, and deck). The data, including probabilities of errors, of error detection, and of failure of the different subsystems conditional on different error states, are obtained through encoding of expert opinion. In this illustration, the opinion of one of the authors (Robert Bea) was used as sole source.[3] His assessments are based on his experience in the oil industry and on in-depth knowledge of different data sets providing statistics about failure types and failure causes (e.g., Refs. 51 and 52). The encoding of the probabilities was done here in several steps: first, elicitation of base rates and conditional probabilities; and, second, checking marginal failure probabilities against available statistics. To assess the probabilities of failure of each subsystem conditional on different levels of error severity, the expert starts from the no-error state, then assesses the multiplicative factors to be applied to this figure to obtain the probability of failure conditional on the next higher level of error severity. The procedure is repeated for each level of severity. Marginal distributions are then computed to verify that the results are compatible with available statistics. Initial assessments showed a tendency to overestimate the contribution of design errors to the failure probability. They were adjusted later by explicit consideration of the effects of errors in the other phases (construction and operation).

4.1. Analytical Model: Error Occurrences and Reliability Effects

Risk assessment for offshore platforms involves a logical analysis of the functions to be performed, identification of the failure modes (i.e., the sequences or conjunctions of failures leading to platform failure), and analysis of the probability of system failure per time

[3] The analysis of a particular platform in a given location requires a specific reliability model based on formal analysis of the local loads. The opinions of several experts should be solicited if necessary.

unit.[53-55] This last step includes the possibility of external events, such as storms that may affect one or more subsystems and act as a common cause of failure. Three functions have to be performed for the platform operation: the anchoring provided by the foundation, the support from the jacket, and the industrial production from the deck. The analysis of failures focuses on the initiating failure (e.g., the foundation, understanding that, in this case, failure of the jacket would necessarily follow). These initiating failures are: failure of the foundation (O), failure of the jacket (A), and failure of the deck (E). They are by definition mutually exclusive and constitute the basic events of the PRA model in its simplest form. Therefore, the probability of failure of the platform (F) is the sum of the probabilities of failure of the basic subsystems as initiating failures. Typical results of a PRA for a whole structure yield an annual probability of platform failure on the order of 2×10^{-3}, allocated as follows among the initiating events: probability of failure of the deck $\approx 10^{-3}$ (about 50%), of the jacket $\approx 6 \times 10^{-4}$ (about 30%), and of the foundation $\approx 4 \times 10^{-4}$ (~20%).[49]

To compute the probability that a platform fails due to undetected errors, we developed an analytical model based on the following events and random variables:

$e_{t,s}$	Error of type t (e.g., gross errors) and severity level s.
e_s	Error of severity level s (including no error: severity 0).
E_i	Initial error state: occurrence of errors in the process (random variable.)
E_f	Final error state after review and correction (random variable.)
D_j	Detection of an error at step j of the review process.
$p(Dj)$	Probability of error detection at step j given that it was not detected before.
C	Error correction.

The probability that an error of given severity level remains at the end of the review process is the probability that an error of this severity initially occurs, is not detected, or is not corrected. The effect is a decrease in the system's capacity to withstand loads and is characterized by the probability of failure conditional on the final error state. The probability of failure of each subsystem is the sum, for all error severity levels, of the joint probabilities of failure and errors. The probability of failure of the whole platform is the sum of the probabilities of (initial) failure of the foundation, the jacket, and the deck. We then allocate it among the different error categories by type and severity level. The equations of the model are thus:

$$p(E_f = E_i = e_s = \sum_i \left\{ p(E_i = e_{i,s}) \times \pi_j [1 - p(D_j | E_i = e_{i,s})] \right\} \quad (1)$$

$$p(X) = \sum_s p(X, e_s) = \sum_s p(E_f = e_s) \times p(X | e_s) \quad (2)$$

for $X = O$, A, or E.

$$p(F) = p(O) + p(A) + p(E) \quad (3)$$

Let Y_i be an initiating event, y a particular level of severity of Y_i, and $f_{Yi}(y)$ the probability density function of the annual maximum value of Y_i.

$$p(X) = \sum_i \left[\int f_{Y_i}(y) \times p(X|y) dy \right] \quad (4)$$

$$p(X|e_s) = \sum_i \left[\int f_{Yi|e_s}(y) \times p(X|y, e_s) dy \right]$$

The occurrence and the severity of some of the initiating events (e.g., wave loads) are independent of errors and, therefore, $f_{Yi|e_s}(y) = f_{Yi}(y)$. Errors, for these initiating events, can affect the fragility of the system, $p(X|y, e_s)$. Other initiators, such as boat collisions, can be influenced by management errors. In this case, both the distribution of loads, $f_{Yi|e_s}(y)$, and the system's fragility, $p(X|y, e_s)$, reflect these errors.

4.2. Design Process and Effect on Platform Reliability

When deciding to design and construct a particular platform, corporate management generally fixes a target production level, the site, type of platform, the time constraints, and the budget. Engineering development chooses the actual type and configuration of the platform. Engineering design decides on the final configuration, design parameters, and inspection and maintenance requirements within the limits set by management and development. Other actors include the contractors and outside participants, such as the regulators, public interest groups, and other oil companies, who have a general interest in the image and performance of the oil industry.

The incentive system is dominated by corporate goals which are set in a rather rigid manner (i.e., with limited and filtered feedback to upper decision levels). Each

level can ask confirmation and clarification regarding particular decisions, but there are strong incentives to stick to the goals and the constraints as set (the ability to meet the goals is a major criterion in salary decisions.) In particular, there is no explicit feedback regarding the shadow price of these constraints (i.e., how much reliability, if any, would be gained by relaxing each of these constraints by one unit). There is little penalty for technical failures, which are rare anyway (mainly a setback in the career of key personnel involved), but there is high penalty for not reaching the corporate goals. One of the key characteristics of the process is the custom of awarding jobs to the lowest bidder, a practice which is viewed as the most effective way to satisfy cost constraints but which may yield poor quality work and decrease system reliability.

The complete process of design, construction, and operations can be divided into specific steps; for example, the preliminary configuration and sizing of platform elements and equipment in the design phase; the installation of jacket, deck, and foundation components in the construction phase; and maintenance procedures in the operation phase. An in-depth study of the process allows identification of the different types of errors that can occur at each step. For simplicity, the only distinction that we make here is between gross errors and errors of judgment, whose probabilities vary according to the subsystem considered and the level of uncertainties involved. The probabilities of detection of these errors depend on their nature and their severity: in general, errors of judgment are less easy to detect and recognize as such than gross errors, and errors of high severity are often easier to detect than errors of low severity. The effects of errors on the probability of system failure depend on their severity.

The design review process is sequential. The first review is performed by the lead engineer, typically competent and knowledgable, but not necessarily someone who has had a long experience in the field. He is, in general, more likely to detect gross errors than errors of judgment. The second review is performed by an experienced engineering manager who may not check the detail of all computations but will detect errors of judgment more easily than the lead engineer. Finally, the constructor may detect an error when actually doing the work on the field. At this late stage, and given the constructor's experience, it is easier to detect gross errors than errors of judgment about which he may have little to say (Table B1).

It was assumed here that, on a global scale, the review process is the same for the different subsystems (foundation, jacket, and deck), although the details of the procedure obviously vary. For example, for the foundation, a significant part of the review may involve the questioning of the assumptions; whereas for the rest of the structure, it may focus more on the verification of the analysis and the computations. On the basis of this analysis, we found that the foundation design review increases the probability of no design error from 0.9–0.922 (which, in relative terms, may look like a modest result) but decreases by 50% the relative rate of high-severity errors (from 0.02–0.01).

For the whole platform, we found that design errors contribute about 40% of the failure probability (92% for the foundation, 50% for the jacket, and 7% for the deck). Of this 40%, 37% can be attributed to gross errors and 63% to errors of judgment that dominate foundation design errors.[56]

4.3. Cumulation of Design, Construction, and Operation Errors

Design errors, however, are only part of the problem. Historical analysis of failures shows that accidents often occur because several errors contribute to weakening a platform, for example, a conjunction of errors in construction and operation. These "resident pathogens"[57] reduce the capacity of the system which becomes susceptible to lower loads. We repeated the previous computations to include explicitly not only design errors but also construction and operations errors. The results are the probabilities of final error states for each subsystem (foundation, jacket, and deck), phase (design, construction, and operation), and severity level (e.g., no design errors, high severity construction error, low severity operation error). We assumed here that although errors can accumulate over the lifetime of a particular subsystem, their occurrences in design, construction, and operation phases are independent among themselves and across subsystems. This simplifying assumption can be questioned for the operations phase (although operation errors generally affect mostly one of the subsystems). For the design and the construction phases, it can be justified by the fact that, to a large extent, different teams design and construct the foundation, the jacket, and the deck.

Examples of construction errors include the possibility that a pile sleeve was only partially grouted (foundation), that the wrong welding rods were used on critical joints (jacket), or the decision to install deck sections in bad weather. Examples of operation errors include a drilling blowout at the foundation level that undermines the foundation, resulting in significant reduction of capacity; for the jacket, the decision not to repair minor dents in braces; and for the deck, the decision to main-

tain production during a fire on the platform, causing an explosion of the production pipeline. Rates of occurrence of construction errors of different types and different severity levels were assessed for each subsystem. The annual distribution for operation errors was assumed to be the same for the three subsystems. The effect of errors on the probability of failure is captured by the probability of failure of each of the subsystems conditional on a level of error (including none), in each of the three phases. Table B2 shows an example of such data for the foundation.

The results include, first, an allocation of the probabilities of failure (for the different subsystems and for the whole platform) among the different levels of dominant errors. Second, the joint distributions of failure states and error severities were computed for each phase of the platform lifetime.[56] Table B3 shows the final results by subsystem (e.g., jacket) and level of *dominant error* (i.e., the most severe one in each combination.) By this definition of dominant error, combinations involving at least one high-severity error are major contributors to the failure probability. Yet *low-severity errors* act as "catalysts" in many such scenarios because they worsen the effect of a concurrent high-severity error. Their contribution to the overall failure probability is thus greater than that of scenarios in which they are dominant. The actual contribution of low-severity errors is thus reassessed separately by computing the overall failure probability with and without them. We find that they actually contribute about 50% of the failure probabilities of the foundation and the jacket, 20% for the deck, and 37% for the whole platform. Thus, low-severity errors are in fact, important contributors to the overall probability of system failure.

In the case of jacket-type offshore platforms, we find that "bad luck" (failures caused by loads far beyond reasonable design criteria) is in fact a small contributor to the failure probability: only 4% of it does not involve errors. Most of the risk can be attributed to errors of various kinds in the different phases. Furthermore, as we discuss below, those that are beyond management control are only a few among many types of possible errors.

4.4. Example of Benefits Assessment: Improvement of the Design Review

For offshore platforms, improvement in the design review can be achieved by the intervention of a certified verifying authority. A high-quality, independent verification process could decrease significantly the probabilities of undetected gross errors as well as errors of judgment. We used the model described above to assess the corresponding gains of reliability based on our expert's assessment of the performance of such an authority. We found that the proposed improvement reduces mostly the probability of failure of the foundation (approximately by a factor of two), to some extent, the probability of failure of the jacket (by about 20%), and reduces little the probability of failure of the deck, which is more susceptible to operations errors than design errors. Altogether, the proposed independent review process could decrease by about half the portion of the failure probability of the whole platform attributable to design errors, thus decreasing the annual probability of system failure by about 20% at a one-time cost of about $100,000.

We compared this result to what it would cost to achieve the same reliability gain through structural reinforcement—for instance, an increase of the number and the strength of jacket members. Base on the rules-of-thumb of the offshore industry, for a structure that costs about $400 million, the cost of reducing the failure probability by a factor of 10 (or 90%) is about 10% ($40 million). Assuming linearity of gains, the cost of reducing the failure probability by 20% is about $9 million. The cost of improving the design review is therefore roughly two orders of magnitude lower than the cost of achieving the same result through structural reinforcement. If the cost of failure is $1 billion and the probability of failure is reduced from 2 to 1.6 $\times 10^{-3}$ per year, the expected value of the annual benefits is $400,000. Whereas these benefits (at 10% discount rate) do not justify a $9 million investment, they obviously justify the initial cost of $100,000 of an independent review. Under the pressure of regulatory agencies and insurance companies, such an independent review has been implemented for several categories of important platforms. However, low-bid practices and "no bad news" philosophies have tended to decrease the potential value of these reviews. Many in engineering management remain skeptical of its effectiveness. The argument is that when they add steel to the structure, they are sure of the result. This illusion of certainty is perhaps due to the belief that the only risk is that of an accident caused by a wave load well beyond the design criteria, not the fact that the structure can have been weakened by error. As we found above, excessive loads account only for about 4% of the failure probability.

5. CONCLUSION

Linking the variables of risk analysis models to some organizational factors can be a useful way to assess the

effects of errors (occurrence and consequences) on system performance. Organizational changes, such as improvement of learning mechanisms or improvement of scheduling to reduce time pressures, may allow reduction of the base rate of errors and increase of the rate of error detection. PRA provides a means of calibrating the impact of potential problems and possible solutions by relating them to the criticality of the functions to be performed by the different components.

In the case of offshore platforms, our analysis provides a way of comparing different approaches to risk management. The results include, first, the relative contributions of errors of different types to the overall probability of failure. Of particular interest is the hidden contribution of low-severity errors. Although high-severity errors seem to dominate the failure probability because they are often the visible trigger of accidents, low-severity errors contribute about 40% of the failure probability because they decrease considerably the capacity of the structure to withstand the effects of high-severity errors. Also, errors of judgment, although less visible than gross errors, appear to contribute more than half of the overall failure probability. Organizations have difficulties observing and correcting them because they are more debatable than gross errors and more likely to survive the normal attempts of their authors to justify their decisions. Finally, our analysis points to cheaper solutions than the technical ones to increase reliability. We show as an example, that the intervention of a certified verifying authority in the design review process can be much less expensive, for the same reliability gain, than adding steel to the structure.

APPENDIX A

PRA Model Structure for the Jacket Only (X-Design or K-Design)

The notations are presented in Table A1.

For the X-design all members have a redundant element. *AX* (failure of the X-design jacket) is the union of all possible ordered pairs of element failures. For the K-design, there is no redundancy (see Fig. 3). *AK* (failure of the K-design jacket) is simply the union of all element failures:

$$AX = \sum_i \sum_{j \neq i} F_i \times F_j \qquad AK = \sum_i F_i \qquad \text{(A1)}$$

Table A1. Notations for the PRA Model

t	Month of the year (time interval)
$\tau(t)$	Mean delay between failure and repair of a member when failure occurs during month t.
A	Jacket failure (*AX* for the X-design; *AK* for the K-design)
F_i	Failure of member i
F_i^0	Failure of member i when all other members are in a nonfailed state
F_i^1	Failure of member i when another member has already failed
$\gamma(t)$	Rate of occurrences of boat collision during month t (barred: mean value)
$\gamma(\tau(t))$	Rate of boat collision during period $\tau(t)$ (barred: mean value)
$B(t)$	Severity of boat collision conditional on occurrence and time of the year (random variable)
$f_{B_t}(b)$	Probability density function for the random variable B during month t
$f_{B\tau(t)}(b)$	Probability density function for the severity of boat collision conditional on occurrence during period $\tau(t)$
$W(t)$	Maximum wave height during month t (random variable)
$f_{W_t}(w)$	Probability density function for the maximum wave height during month t
$f_{W\tau(t)}(w)$	Probability density function for the maximum wave height during period $\tau(t)$
R_i	Resistance of element i
a_i	Influence coefficient: $a_i w$ or $a_i b$ represents the force on element i due to wave loads w or force of boat collision b. This coefficient may take on several values according to the state of the rest of the structure
a_i^0	Value of a_i when the rest of the structure is intact
a_i^1	Value of a_i when another member has already failed

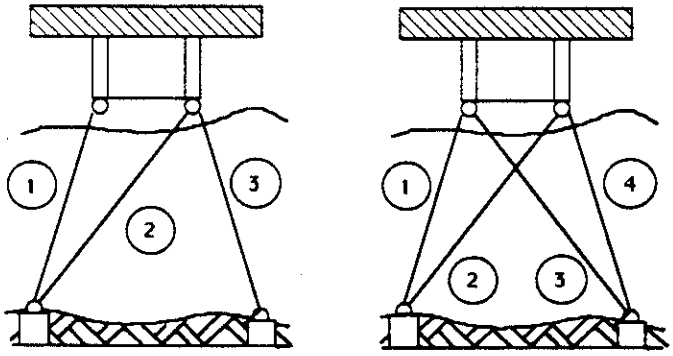


Fig. 3. Schematic representation of two jacket configurations: K-design (left) and X-design (right).

X-Type Jacket

Failures of the different elements may not occur simultaneously. When one of the members fails alone,

the loads shift among the remaining members of the structure. The probability of failure of each element conditional on a particular level of load thus depends on the state of the other members. Thus, two classes of failure scenarios are: two redundant members are destroyed by the same initiating event (e.g., the same wave or the same storm) leading to jacket failure, or by a second event with a delay if one member fails first and another one fails in a consecutive event before the first member has been repaired. The two initiating events chosen for this illustration (boat collisions and waves) are dependent. Therefore, following the loss of a member in the winter, the management may face a tradeoff between the risk of boat collision when bringing repair equipment on board, and the risk due to another storm that may destroy a second member (and therefore the jacket) before the first member is fixed.

The six scenarios of X-type jacket failures are thus:

- Scenario 1: The same wave or storm destroys two members (wave-wave).
- Scenario 2: The same boat collision destroys two members (boat-boat).
- Scenario 3: A wave destroys one member; a boat collision destroys another member during the delay between the first failure and repair of the failed member (wave-delay-boat).
- Scenario 4: A boat collision destroys one member; a wave destroys another member during the delay between the first failure and repair of the failed member (boat-delay-wave).
- Scenario 5: A wave destroys one member; a second wave destroys another member during the delay between the first failure and repair of the failed member (wave-delay-wave).
- Scenario 6: A boat collision destroys one member; a second boat collision destroys another member during the delay between the first failure and repair of the failed member (boat-delay-boat). [Note that we consider that the probability of simultaneous failures of two members due to wave load for one and boat collision for the other as negligible.]

The wave loads vary with the time of the year, and the rate and severity of boat collision both vary with the waves. The time of the year is thus chosen here as the independent variable. It is assumed that the delay between failure of a member and its repair is a function of the season, and that this period can be characterized by the same weather and wave heights as the month in which it starts. For failures due to wave loads, it is also assumed that failure of a member during a given period is caused by the wave of maximum height during the considered period [either the month t or the repair delay $\tau(t)$ during that month]. Let $p_k(A,t)$ be the probability of failure of the X-design jacket during month t for each of the six failure scenarios (index k):

$$
\begin{aligned}
p_1(A,t) &= \sum_i \sum_{j \neq i} \int p(F_i^0|w) \times p(F_j^1|w) \times f_{W_t}(w)dw \\
p_2(A,t) &= \bar{\gamma}(t) \sum_i \sum_{j \neq i} \int p(F_i^0|b) \times p(F_j^1|b) \times f_{B_t}(b)db \\
p_3(A.t) &= \sum_i \sum_{j \neq i} \Big[\int p(F_i^0|w) \times \Big\{ 1 - p(F_j^1|w) \Big\} f_{W_t}(w)dw \\
&\quad \times \bar{\gamma}(\tau(t)) \int p(F_j^1|b) f_{B_t}(b)db \Big] \\
p_4(A.t) &= \sum_i \sum_{j \neq i} \Big[\bar{\gamma}(t) \int p(F_i^0|b) \times \{1 - p(F_j^1|b)\} f_{B_t}(b)db \\
&\quad \times \int p(F_j^1|w) f_{W_{\tau(t)}}(w)dw \Big] \\
p_5(A.t) &= \sum_i \sum_{j \neq i} \Big[\int p(F_i^0|w) \times \{1 - p(F_j^1|w)\} f_{W_t}(w)dw \\
&\quad \times \int p(F_j^1|w) f_{W_{\tau(t)}}(w)dw \Big] \\
p_6(A.t) &= \sum_i \sum_{j \neq i} \Big[\bar{\gamma}(t) \int p(F_i^0|b) \times \{1 - p(F_j^1|b)\} f_{B_t}(b)db \\
&\quad \times \bar{\gamma}(\tau(t)) \int p(F_j^1|b) f_{B_t}(b)db \Big]
\end{aligned}
\tag{A2}
$$

The probability of failure of the X-design jacket during month t is the sum of the probabilities failure attributable to the six failaure scenarios described above:

$$p(A,t) = \sum_k p_k(A,t) \tag{A3}$$

K-Type Jacket

In this case, there is no redundancy. The failure modes are therefore: failure of member 1, or member 2, or member 3. The probability of failure of the jacket during month t is thus:

$$
p(A,t) = \sum_i \Big\{ \int p(F_i^0|w) \times f_{W_t}(w)dw + \bar{\gamma}(t) \int p(F_i^0|b) \times f_{B_t}(b)db \Big\} \tag{A4}
$$

For both designs, the probability of failure of the jacket during the whole year (at least one event) is:

$$p(A) = 1 - \prod_t [1 - p(A,t)] \tag{A5}$$

The probabilities of failure of the different members are functions of their resistances and of the loads applied

to them, given the status of the other member. Failure occurs when the resistance of element i is less than the force to which it is subjected, given that the rest of the structure is intact:

$$\begin{aligned} F_i^0|w &= R_i < a_i^0 w \\ F_i^0|b &= R_i < a_i^0 b \\ F_j^1|w &= R_j < a_j^1 w \\ F_j^1|b &= R_j < a_j^1 b \end{aligned} \quad \text{(A6)}$$

The resistance R_i for members in tension (e.g., members 2 and 3 in Fig. 2) is:

$$R_i = a_S \times f_Y \quad \text{(A7)}$$

The reliability of the jacket can thus be expressed as a function of (1) its configuration, (2) the cross-section of its members, (3) the quality of the steel, and (4) in addition to the terms of the previous equations, the resistance of the joints.[4]

Technical Causes of Failure

Examination of the inputs of the PRA model for a jacket allows systematic identification of the technical (first-level) causes of failure. Table A2 shows this correspondence for the jacket.

Decision or Action That Leads to Technical Causes of Failures

The technical failures identified in Table A2 can, in turn, be related to either decisions or human actions that cause either an increase of the probability of the initiating events, or a decrease of the system's capacity. These decisions or action can be either linked to organizational errors (with or without classic human errors) or to human errors (rooted or not in an organizational feature). These errors are classified here by phase of occurrence (design, construction, or operation), failure cause, and PRA input. In addition, the severity of the error influences the effect on the corresponding input.

[4] Joints fail mainly in three ways: punch-through or pull-out (e.g., a member in compression punches through or a member in tension pulls out of one of the legs), buckling (either of the member or of the leg), and fatigue in the walls (caused by stress concentration or hot spots). The resistance of the joints thus depends on the configuration of legs and members, on the cross-section of the elements, the quality of the weldings, the quality of the steel, and the resistance to corrosion provided by cathodic protection.

Table A2. Technical Failures Associated with the Basic Inputs of the PRA Model for an X-Type Jacket

PRA inputs	Technical cause of failure
1. $f_{W_t}(w)$	Wave heights cause forces in the structure that exceed the capacity of one or more member during month t
2. $f_{W_{\tau(t)}}(w)$	Wave heights cause forces in the weakened structure (i.e., following failure of one of the members) that exceed the capacity of one or more member(s) during the delay between first failure (that occurred at month t) and repair
3. $\gamma(t)$	Occurrence of boat collisions during month t
4. $\gamma(\tau(t))$	Occurrence of boat collisions during the delay between first failure (that occurred at month t) and repair
5. $f_{B_t}(b)$	Boat collision during month t cuases forces in the structure that exceed the capacity of one or more member(s)
6. $f_{B_{\tau(t)}}(b)$	Boat collision causes forces in the weakened structure (i.e., following failure of one of the members) that exceed the capacity of one or more member(s) during the delay between first failure (that occurred at month t) and repair
7. R_i	Insufficient resistance of member: 7a: cross-section is too small (by design or by corrosion), or 7b: yield stress of the steel is too low
8. a_i^0, a_j^1	Configuration causes allocation of forces within the structure that creates excessive loads on one or more member(s)

Organizational Roots of Decisions and Actions

Each of the decisions and actions identified in Table A3 can be related to organizational features that shape that decision. For each of the three phases, these factors can be identified as:

Design:

- design constraints and goals
- designer's competence and philosophy
- design procedures (ex: compatibility of platform and boat approach system)
- design review process (procedures, incentives, resource constraints)

Construction:

- constraints (material, time, etc.)
- incentives and rewards: penalties for delays
- selection and qualification of personnel; philosophy of the constructor
- quality control procedures

Operations:

- production decisions (production level; when to stop production)

Table A3. Decisions and Actions Linked to Technical Failures for a Schematic X-Type Jacket[a]

Technical cause of failure	Decision or action in Phases *D* (design), *C* (construction) or *O* (operation)
1. Wave load during month t	*D*: Choice of platform configuration (*D*1) and design parameter (sizing) (*D*2)
	O: Decision to operate in bad weather (*O*1)
2. Wave load during repair delay	*O*: Detection of initial member failure (*O*3)
3. Boat collision during month t	*D*: Design of boat approach systems (*D*3)
	O: Training of boat masters (*O*4); decision to let boat come close to platform given weather (*O*5); procedures of boat operations (*O*6)
4. Boat collision during repair delay	*D*: Configuration of platform (*D*1) and approach systems (D3)
	O: Decision to let boat approach a *weakened* platform in bad weather (*O*3); training of boat masters (*O*4)
5. Force of boat collision during month t	*O*: Choice of the type of boat allowed to approach platform given weather (*O*7); procedures of boat maneuver (*O*6); training of masters (*O*4)
6. Force of boat collision during repair delay	*O*: Procedure of detection of failure of initial member (*O*2); choice of the type of boat that is allowed to approach a *weakened* platform given weather (*O*3); procedures of approach and maneuver around damaged structure (*O*3); training of masters (*O*4)
7a. Cross-section of members is too small	*D*: Error in the sizing of members (*D*2)
	C: Errors in construction: error of sizing (*C*1); defective welding (*C*2); wrong configuration at construction stage (*C*3)
	O: Delay in maintenance operations that causes corrosion (*O*8). Failure to observe corrosion effects (*O*9). Failure to interrupt production to repair corrosion damage (*O*10)
7b. Yield stress of the steel is too low	*D*: Choice of the wrong grade of steel (*D*4)
	C: Substitution of steel at construction time (for reason of cost or unavailability) (*C*4)
8. Allocation of forces within the structure	*D*: Wrong configuration and sizing in design (*D*1, *D*2)
	C: Wrong configuration and sizing in construction (*C*1)
	O: Failure to observe and repair decrease in capacity of system in operations (*O*2; *O*3; *O*5)

[a]Entries 1–6 relate to loads, 7 and 8 the capacity. Decisions and actions are labeled by phase and numbered by an index (ex: D5).

- inspection and maintenance of the structure after member failure (due to wave or boat collision) for corrosion
- procedures of production on a weakened platform
- boat operations around regular and weakened structure.

Example of Assessment of Procedures of Boat Operations Around a Platform

1. Decisions and actions:

   O3: procedure for repair of platform damage (to approach damaged structure); choice of boat types allowed to approach a damaged structure.

   O4: training of boat pilots.

   O5: procedure of boat operation around intact structures.

   O6: procedure of boat operation around damaged structures.

2. Variables affected in the PRA model:

   $\gamma(t)$: Rate of boat collision during month t.

   $\tau(t)$: Mean delay between failure and repair when failure occurs during month t.

   $\gamma(\tau(t))$: Rate of boat collision during repair delay.

   $B(t)$: Force of boat collision during month t and during repair delay.

A modification of a procedure can be characterized by a variation of the PRA inputs. The quantification of this variation requires expert assessment or statistical estimation of these inputs under different management rules. For example, restriction of some of the procedures of boat operation around an intact structure can be char-

Table B1. Probabilities of Detection of Design Errors by the Successive Reveiwers and Probabilities of Error Correction Given Detection (Illustrative values)

Type of error	Engineering			Corrective action
	Lead engineer	manager	Constructor	
Gross error				
High severity	0.45	0.8	0.7	0.9
Low severity	0.20	0.65	0.4	0.6
Error of judgment				
High severity	0.20	0.5	0.1	0.6
Low severity	0.05	0.3	0.01	0.2

acterized (1) by a reduction of the rate of boat collision and (2) by a reduction of the force of such collision if it occurs. More specifically, restriction of boat maneuver around platforms at certain times of the year allows computation of the probabilities of failure by setting the rate of boat collision to 0 for the corresponding months. For the X-type structure, the decrease of the probability of failure due to a variation of boat-related procedures is:

$$\Delta p(AX,t) = \Delta p_2(AX,t) + \Delta p_4(AX,t) + \Delta p_6(AX,t) \quad \text{(A8)}$$

in which the Δp_i's represent the variation of the probabilities of the corresponding failure scenarios. For example, a procedure that decreases by $\Delta\bar{\nu}(t)$ the mean rate of boat collision with an intact structure and for each month t, reduces the probability $p(AX,t)$ by:

$$\Delta p(AX,t) = \Delta\bar{\nu}(t)\sum_i\sum_{j\neq i}\int p(F_i^0|b) \times p(F_j^1|b)\times f_{B_t}(b)db + \Delta\bar{\nu}(t)\sum_i\sum_{j\neq i}\left[\int p(F_i^0|b)\times\{1 - p(F_j^1|b)\}f_{B_t}(b)db\right] \quad \text{(A9)}$$

Table B2. Example of Data: Annual Probability of Failure of the Foundation Conditional on Levels of Severity for Design Errors, Construction Errors, and Operations Errors[a]

FOUNDATION						
Design errors	*Probability*	Construction errors	*Probability*	Operation errors	*Probability*	Failure probability
NDE	0.9220	NCE	0.9220	NOE	0.85	E-5
				LOE	0.10	2E-5
				HOE	0.05	4E-5
		LCE	0.0676	NOE	0.85	6E-5
				LOE	0.10	E-4
				HOE	0.05	2E-4
		HCE	0.0104	NOE	0.85	E-3
				LOE	0.10	4E-3
				HOE	0.05	E-2
LDE	0.0676	NCE	0.9220	NOE	0.85	E-4
				LOE	0.10	5E-4
				HOE	0.05	E-3
		LCE	0.0676	NOE	0.85	4E-4
				LOE	0.10	2E-3
				HOE	0.05	5E-3
		HCE	0.0104	NOE	0.85	E-2
				LOE	0.10	2E-2
				HOE	0.05	6E-2
HDE	0.0104	NCE	0.9220	NOE	0.85	E-2
			0.10	LOE	0.10	2E-2
			0.05	HOE	0.05	6E-2
		LCE	0.0676	NOE	0.85	0.2
				LOE	0.10	0.4
				HOE	0.05	0.7
		HCE	0.0104	NOE	0.85	0.4
				LOE	0.10	0.7
				HOE	0.05	0.9

[a]NDE, no design error; LDE, low-severity design error; HDE, high-severity design error; NCE, no construction error; LCE, low-severity construction error; HCE, high-severity construction error; NOE, no operation error; LOE, low-severity error; HOE, high-severity operation error.

Table B3. Example of Results: Joint and Conditional Probabilities of Failure of the Jacket Given Different Types of Errors

Jacket	Annual Failure Probability:	$p(A) = 6.06 \times 10^{-4}$
	Design	
Probability of failure and design errors	Failure probability conditional on design errors	Probability of design errors
$p(A, \text{NDE}) = 3.07\text{E-}4$	$p(A\|\text{NDE}) = 3.22\text{E-}4$	$p(\text{NDE}) = 0.9547$
$p(A, \text{LDE}) = 1.99\text{E-}4$	$p(A\|\text{LDE}) = 4.86\text{E-}3$	$p(\text{LDE}) = 0.0401$
$p(A, \text{HDE}) = 9.95\text{E-}5$	$p(A\|\text{HDE}) = 1.91\text{E-}2$	$p(\text{HDE}) = 0.0052$
Total: $= p(A)$		
	Construction	
Probability of failure and constr. errors	Failure probability conditional on constr. errors	Probability of constr. errors
$p(A, \text{NCE}) = 1.74\text{E-}4$	$p(A\|\text{NCE}) = 1.82\text{E-}4$	$p(\text{NCE}) = 0.9547$
$p(A, \text{LCE}) = 2.15\text{E-}4$	$p(A\|\text{LCE}) = 5.23\text{E-}3$	$p(\text{LCE}) = 0.0401$
$p(A, \text{HCE}) = 2.18\text{E-}4$	$p(A\|\text{HCE}) = 4.17\text{E-}2$	$p(\text{HCE}) = 0.0052$
Total: $= p(A)$		
	Operations	
Probability of failure and operations errors	Failure probability conditional on operations errors	Probability of operations errors
$p(A, \text{NOE}) = 3.04\text{E-}4$	$p(A\|\text{NOE}) = 3.57\text{E-}4$	$p(\text{NOE}) = 0.85$
$p(A, \text{LOE}) = 1.15\text{E-}4$	$p(A\|\text{LOE}) = 1.15\text{E-}3$	$p(\text{LOE}) = 0.10$
$p(A, \text{HOE}) = 1.88\text{E-}4$	$p(A\|\text{HOE}) = 3.76\text{E-}3$	$p(\text{HOE}) = 0.05$
Total: $p(A)$		

$$\times \int p(F_j^1|w) f_{W(t)}(w)dw \Bigg]$$

$$- \Delta\bar{\gamma}(t) \sum_i \sum_{j \neq i} \Bigg[\int p(F_i^0|b)$$

$$\times \{1 - p(F_j^1|b)\} f_B(b)db \times \bar{\gamma}(\tau(t)) \int p(F_j^1|b) f_B(b)db \Bigg]$$

By contrast, for a K-type structure, an improvement of procedure that decreaes by $\Delta\bar{\gamma}(t)$ the mean rate of boat collision with an intact structure for each month t, decreases the probability of failure by:

$$\Delta p(AK, t) = \sum_i \Delta\bar{\gamma}(t) \int p(F_i^0|b) \times f_B(b)db \qquad \text{(A10)}$$

For K-structures that lack redundancies, procedures designed to avoid member failures due to boat collisions are simply a matter of survival. In this case, the PRA approach thus allows linking the choice of an operation procedure to that of a design configuration.

APPENDIX B

See Tables B1 through B3.

REFERENCES

1. C. B. Brown, and X. Yin, "Errors in Structural Engineering." *Journal of Structural Engineering* **114**, 2575–2593 (1988).
2. E. J. Henley, and H. Kumamoto, *Reliability Engineering and Risk Assessment* (Prentice-Hall Inc., Englewood Cliffs, New Jersey, 1981; Cambridge University Press, Cambridge, U.K., 1981).
3. Presidential Commission on the Space Shuttle Challenger Accident (Washington, D.C., 1986).
4. M. E. Paté-Cornell, "Organizational Factors in Reliability Models," *Proceedings of the Annual Meeting of the Society for Risk Analysis* (Washington, D.C., 1988).
5. M. E. Paté-Cornell, "Organizational Aspects of Engineering System Reliability: The Case of Offshore Platforms," *Science* 1210–1217 (1990).
6. S. Arueti, and D. Okrent, "Combining Objective and Subjective Techniques for Assessing Quality Management," *Proceedings of SMiRT9 1987* (Lausanne, Switzerland, 1987).
7. B. Ellingwood, Design and Construction Error Effects on Structural Reliability, *Journal of Structural Engineering* **113**, 409–422 (1987).
8. J. S. Wu, G. E. Apostolakis, and D. Okrent, "On the Inclusion of Organizational and Managerial Influences in Probabilistic Safety Assessments of Nuclear Power Plants, *Proceedings of the 1989 Annual Meeting of the Society for Risk Analysis* (San Francisco, 1989).
9. T.-M Hsieh, and D. Okrent, "On Design Errors and System Deg-

radation in Seismic Safety," *Proceedings of SMiRT4* (San Francisco, California, 1977).
10. M. K. Ravindra, "Gross Design and Construction Errors, and Seismic Risk Studies," *Nuclear Engineering and Design* **110**, 255–263 (1988).
11. T. R. La Porte, *High Reliability Organization Project* (University of California, Berkeley, California, 1988).
12. K. H. Roberts, and D. M. Rousseau, "Research in Nearly Failure-free, High Reliability Organizations: Having The Bubble," *IEEE Transactions on Engineering Management* **36**, 132–139 (1989).
13. C. Perrow, *Normal Accidents* (Basic Books, New York, 1984).
14. W. R. Freudenburg, "Perceived Risk, Real Risk: Social Science and the Art of Probabilistic Risk Assessment," *Science* **242**, 44–49 (1988).
15. The Hon. Lord Cullen, *The Public Inquiery into the Piper Alpha Disaster*, Vols. 1 and 2 (Report to Parliament by the Secretary of State for Energy by Command of Her Majesty, November 1990).
16. J. G. March, and H. A. Simon, *Organizations* (John Wiley & Sons, New York, 1958).
17. K. J. Arrow, *Decision and Organization* (North Holland, Amsterdam, The Netherlands, 1972).
18. H. A. Simon, *Administrative Behavior* (Free Press, New York, 1976).
19. J. G. March, and J. P. Olsen, *Ambiguity and Choice in Organizations* (Universitetsforlaget, Bergen, Norway, 1976).
20. J. G. March, *Decisions in Organizations* (Blackwell, New York, 1988).
21. J. G. March, and Z. Shapira, "Managerial Perspective on Risk and Risk Taking," *Management Science* **33**, (1988).
22. K. E. Weick, "Organizational Culture as a Sources of High Reliability," *California Management Review* (1987).
23. D. D. Woods, E. M. Roth, and H. Pople, "Modeling Human Intention Formation for Human Reliability Assessment," *Reliability Engineering and System Safety* **22**, 169–200 (1988).
24. J. Rasmussen, K. Duncan, and J. Leplat (eds.), *New Technology and Human Error* (J. Wiley, Chichester, 1987).
25. D. A. Norman, "Characterization of Action Slips," *Psych. Rev.* **88**, 1–15 (1981).
26. J. Rasmussen, and W. B. Rouse (eds.), *Human Detection and Diagnosis of System Failures* (Proceedings of a NATO Symposium, Roskilde, Denmark, 1980; Plenum, New York, 1981).
27. J. T. Reason, "The Human Contribution to 'Organizational Accidents,'" *Second World Bank Workshop on Safety Control and Risk Management* (Karlstad, Sweden, November 1989).
28. J. T. Reason, "Modeling the Basic Error Tendencies of Human Operators," *Reliability Engineering and System Safety* **22**, 137–153 (1988).
29. J. T. Reason, *Human Error* (Cambridge University Press, New York, 1990).
30. R. M. Cyert, and J. G. March, *A Behavioral Theory of the Firm* (Prentice-Hall, Englewood Cliffs, New Jersey, 1963).
31. E. Hollnagel, G. Mancini, and D. D. Woods (eds.), *Cognitive Engineering in Complex Dynamic Worlds* (Academic Press, London, 1988).
32. L. P. Goodstein, H. B. Andersen, and S. E. Olsen (eds.), *Tasks, Errors and Mental Models* (Taylor and Francis, London, 1988).
33. J. Rasmussen, *Information Processing and Human-Machine Interaction* (North Holland, New York, 1986).
34. D. Kahneman, P. Slovic, and A. Tversky, *Judgment Under Uncertainty: Heuristics and Biases* (Cambridge University Press, New York, 1982).
35. B. Turner, and M. R. Williams, *Management Handbook For Engineers and Technologists* (Business Books, London, U.K., 1983).
36. H. A. Simon, *Models of Bounded Rationality* (MIT Press, Cambridge, Massachusetts, 1982).
37. B. Levitt, and J. G. March, "Organizational Learning," *Annual Review of Sociology* **14**, 319–340 (1988).
38. E. L. Janis, *Victims of Group Think* (Houghton Mifflin, Boston, 1972).
39. B. Fischhoff, S. Lichtenstein, P. Slovic, S. Derby, and R. Keeney, *Acceptable Risk* (Cambridge University Press, New York, 1981).
40. J. G. March, "Variable Risk Preferences and Adaptive Aspirations," *Journal of Economic Behavior and Organizations* **9**, 5–24 (1988).
41. W. G. Carson, *The Other Price of Britain's Oil: Safety and Control in the North Sea* (Rutgers University Press, New Brunswick, New Jersey, 1982).
42. C. Heimer, "Social Structure, Psychology, and the Estimation of Risk," *Annual Review of Sociology* **14**, 491–519 (1988).
43. A. Tversky, and D. Kahneman, "The Framing of Decisions and the Psychology of Choices," *Science* **211**, 453–458 (1981).
44. D. Kahneman, and D. Lovallo, "Timid Decisions and Bold Forecasts," (Presentation at the Conference on Fundamental Issues in Strategy, Silverado, 1990).
45. R. Dawes, Personal communication (1990).
46. W. Rouse, *System Design* (North Holland, New York, 1987).
47. S. Kaplan, "On the Inclusion of Precursors and Near-miss Events in Quantitative Risk Assessments: A Bayesian Point of View and a Space Shuttle Example," *Journal of Reliability Engineering and System Safety* **27**, 103–115, (1990).
48. A. L. Stinchcombe, and C. A. Heimer, *Organization Theory and Project Management. Administering Uncertainty in Norwegian Offshore Oil* (Norwegian University Press, Oslo, Norway, 1985).
49. R. G. Bea, "Reliability Considerations in Offshore Platform Criteria," *Journal of the Structural Division of the American Society of Civil Engineers* **106**, (ST9) (1980).
50. B. Staw, "The Escalation of Commitment to a Course of Action," *Academy of Management Review* **6**, 1–39 (1977).
51. OCB (Offshore Certification Bureau), Comparative Safety Evaluation of Arrangements for Accommodating Personnel Offshore (Report OTN-88-175, December 1988).
52. Veritec, The Worldwide Offshore Accident Data Bank (WOAD) (annual reports through 1988, Oslo, Norway).
53. Royal Norwegian Council for Scientific and Industrial Research (Risk Assessment Report of the Norwegian Offshore Petroleum Activities, Oslo, Norway, 1979).
54. U.S. Department of Commerce, National Bureau of Standards, *Application of Risk Analysis to Offshore Oil and Gas Operations* (Proceedings of and International Workshop, NSB Special Publications 695, Washington D.C., May 1985).
55. H. Nordal, C. A. Cornell, and A. Karamchandani, "A Structural System Reliability Case Study of an Eight-leg Steel Jacket Offshore Production Platform," *Proceedings of the Marine Structural Reliability Symposium* (SNAME, Arlington, Virginia, 1987).
56. M. E. Paté-Cornell, and R. G. Bea, "Organizational Aspects of Reliability Management: Design, Construction, and Operation of Offshore Platforms" (Research Report No. 89-1, Department of Industrial Engineering and Engineering Management, Stanford University, Stanford California, 1989).
57. J. T. Reason, "Resident Pathogens and Risk Management," *First World Bank Workshop on Safety Control and Risk Management* (Washington D.C., 1988).

OTC 7121

Human and Organizational Error in Operations of Marine Systems: Occidental Piper Alpha and High-Pressure Gas Systems on Offshore Platforms

W.H. Moore and R.G. Bea, U. of California

This paper was presented at the 25th Annual OTC in Houston, Texas, U.S.A., 3-6 May 1993.

ABSTRACT

This paper establishes methodologies for formulating qualitative and quantitative models to identify and evaluate the impacts of human and organizational errors (HOE) on offshore operations. Qualitative and quantitative models of simultaneous production and maintenance related to Piper Alpha *disaster are used as a case study to illustrate the identification and assessment of alternatives to minimize the effects of HOE in high pressure gas system operations. Quantitative data is limited in availability and detail to assist evaluations of HOE management alternatives. However, when this data is combined with a realistic structuring of the human, organization, and system components of marine systems, then useful results can be developed to guide judgments to improve the reliability of these systems.*

INTRODUCTION

Available data on the performance of marine systems during the last two decades indicates that approximately 65% of catastrophic marine related accidents are the result of compounded human and organizational errors (HOE) during operations.

References and tables at end of paper.

In spite of this experience, there is no structured, general, qualitative and quantitative approach to assist engineers, operators, and regulators in the evaluation of alternatives to help minimize human and organization errors in marine systems. To be able to realize significant improvements in the reliability of marine systems, guidelines and procedures should be established to include explicit consideration of human and organizational errors as an integral part of the design, construction, and operation of offshore structures.[1]

This paper examines methodologies used to mitigate the impacts of HOE during operations of offshore structures. A case study of the *Piper Alpha* disaster is used to illustrate examination of the effects of HOE in simultaneous offshore maintenance and production operations of high pressure gas systems. Influence diagrams are developed to illustrate the interactions of the multiple accident events, decisions, and actions and to evaluate their contributing HOE factors. The models are used to examine HOE management alternatives to reduce the likelihood of failure events.

BACKGROUND

Development of accident framework models is the third of five tasks in the Joint Industry Project titled *Management of Human Error in Operations of Marine*

Systems conducted by the Department of Naval Architecture & Offshore Engineering at the University of California at Berkeley during the past three years. The five tasks are:

(1) Identify, obtain and analyze well documented case histories and databases of tanker and offshore platform accidents whose root causes are founded in HOE.

(2) Develop a classification framework for systematically identifying and characterizing the various types of HOE.

(3) Develop general analytical frameworks based on a study of real-life case histories of major marine accidents to characterize how HOE interact to cause such accidents.

(4) Formulate quantitative analyses for the case histories based on probabilistic risk analysis (PRA) procedures using influence diagrams. Perform quantitative analyses to verify that the analyses can reproduce the results and implications from the case histories and general marine casualty statistics.

(5) Investigate the effectiveness of various alternatives to reduce the incidence and mitigate the consequences of HOE's. Evaluate the costs and benefits in terms of risk reduction (products of likelihood and consequences).

The *Piper Alpha* and the *Exxon Valdez* accidents were chosen as the two case histories and qualitative analytical frameworks developed for each of the accidents [2,3]. The *Piper Alpha* and *Exxon Valdez* accidents were selected because of the quality, completeness, accessibility, and availability of information related to the accident events.

The *Piper Alpha* accident resulted in 106 specific recommendations leading to changes in United Kingdom Offshore Continental Shelf (OCS) legislation and regulation[4] These recommendations have lead to a requirement for the performance of Safety Case Studies on platforms in the U. K. sector of the North Sea. The *Piper Alpha* disaster has had world-wide effects on the design and operations of offshore platforms.[5]

ACCIDENT MODELS

There are four principal steps in development of a post-mortem analysis:

(1) structuring the relevant events, decisions, and actions specific to the accident scenario,

(2) applying human and organizational error classifications to identify contributing factors,

(3) development of models representative of accident classes of which the accident falls within that class, and

(4) determination of a general set of contributing HOE causes related to events, decisions and actions related to the class of accidents.

Models Representing Classes of Accidents

A primary objective is to develop and verify Probabilistic Risk Analysis (PRA) models for operations of offshore platforms to include explicit evaluation of HOE. The general method is to integrate elements of traditional probabilistic process analysis with HOE analysis to assess the probability of system failure.[1,6]

A probabilistic model of the process includes determining the set of possible initiating accident events (in_i) and final states ($fist_m$) of the system. The probability of loss of components of the system can be represented by:

$$p(loss_k) = \sum_i \sum_m p(in_i)\, p(fist_m|in_i)\, p(loss_k|fist_m) \qquad \forall\, k. \quad \ldots\ldots(1)$$

The model is expanded to include relevant decisions and actions (A_n) constituting an exhaustive and mutually exclusive set of decisions or actions affecting the system at different stages during the lifetime of the platform. These decisions and actions can be examined from the front-line operating crew level through top-level management:

$$p(loss_k) = \sum_i \sum_m \sum_n p(A_n)\, p(in_i|A_n)\, p(fist_m|in_i, A_n)\, p(loss_k|fist_m, A_n) \quad \forall\, k. \quad \ldots\ldots(2)$$

The effects of organizational factors on the risk are determined through examining the probabilities of actions and decisions conditional on relevant organizational factors (O_h). The probabilities of various degrees of loss can be examined conditional upon different contributing organizational factors:

$$p(loss_k|O_k) = \sum_i \sum_m \sum_n p(A_n|O_k)\, p(in_i|A_n)\, p(fist_m|in_i, A_n)\, p(loss_k|fist_m, A_n) \quad \ldots\ldots(3)$$

Influence Diagrams

One method of developing accident framework models for PRA analysis is through the use of *influence diagrams*. Influence diagramming provides flexibility in defining the relationships and correlation of system and HOE components and in examining HOE management alternatives. There are distinct advantages to influence diagrams as an alternative to standard event/fault tree analyses to assess conditional probabilities required to determine unconditional probabilities of specified target events.[7]

In standard decision tree analysis, decisions are based on all preceding aleotory and decision variables.[8] However, not all information is necessarily available to a decision maker. In addition, information may originate from indirect sources or not the specific order a decision tree is modeled. It is not necessary for all nodes be totally ordered in an influence diagram. This allows for decision makers who agree on common based states of information, but differ in ability to observe certain variables in the diagram modeling.[8]

The primary components of an influence diagram are (refer to Figure 4): *decision* and *chance nodes, arrows, deterministic nodes*, and *value nodes*.[9]

Decisions are represented by square nodes which can be a continuous or discrete variable or set of decision alternatives. Uncertain events or variables are represented by circular or oval chance nodes. Chance nodes can be continuous or discrete random variables or a set of events. Arrows indicate relationships between nodes in the diagram. Arrows entering a chance node signify the probability assignments of the node are conditional from where the arrow originated. Deterministic nodes depend deterministically upon its predecessors. A value node is designated as: "the quantity whose certain equivalent is to be optimized by the decisions". Only one node may be designated in the diagram and are represented by a rounded edge double-border rectangle.

Structuring Relevant Events, Decisions and Actions

To establish accident events, decisions, actions, and causes a preliminary diagram representation of the accident is constructed. The diagram is not an influence diagram per se since no probabilities are assessed, but a representation of the accident factors which occurred. The purpose of the diagram is to assist the user in establishing the relevant contributing factors unique to the specific accident sequence (see Fig. 2). In addition, it assists the user in identifying critical areas where: (a) risk and consequences may be managed and controlled, or (b) further detailed study may be warranted.

The modeling process begins with a specific accident model formulation and results in the development of an influence diagram that encompasses the class of accidents in which the post-mortem model is a representative. The model development (and preliminary model representations) should be the effort of a group of experts. Discussion of differences in opinion of relationships between events and their causes illicit the development of more realistic models.[16]

The modeling process includes the structuring of a target event which is the final result of contributing events, decisions, and actions (e.g. platform fire, loss of life or platform, etc.). The first step is to represent dependencies between relevant events decisions and actions which may be categorized into three states:

(1) ***Contributing/underlying events, decisions and actions***: Contributing/ underlying events are those occurring prior to the initiating accident event contributing to the reduction of reliability or increase of risk for the system (decision to simultaneously produce and conduct process maintenance on *Piper Alpha*).

(2) ***Initiating/direct accident events, decisions, and actions***: The immediate accident event(s), decisions, and actions resulting in the casualty (the initial explosions and fires were the result unfinished maintenance of condensate pumps in Module C).

(3) ***Compounding events, decisions and actions***: The events, decisions, and actions which lead to compounding of accident consequences (increasing the flow of gas to *Piper Alpha* from satellite platforms *Claymore* and *Tartan*).

HOE CLASSIFICATION

Based on a study of several hundred well documented accident reports involving marine systems and a review of several proposals for description

of HOE Moore & Bea have developed an HOE classification for marine accidents (Fig. 1).[10] The classification identifies four major components: (a) the physical system, (b) the human front line operators of the system, (c) the industry organization that oversees and directs the design, construction, and operation of the system and (d) the regulatory groups that provide the public safeguards and interests representation associated with the marine system. Thirteen mutually exclusive elements comprise the HOE classification; two of these (commitment to safety and resources provided for safety) pervade the four components.

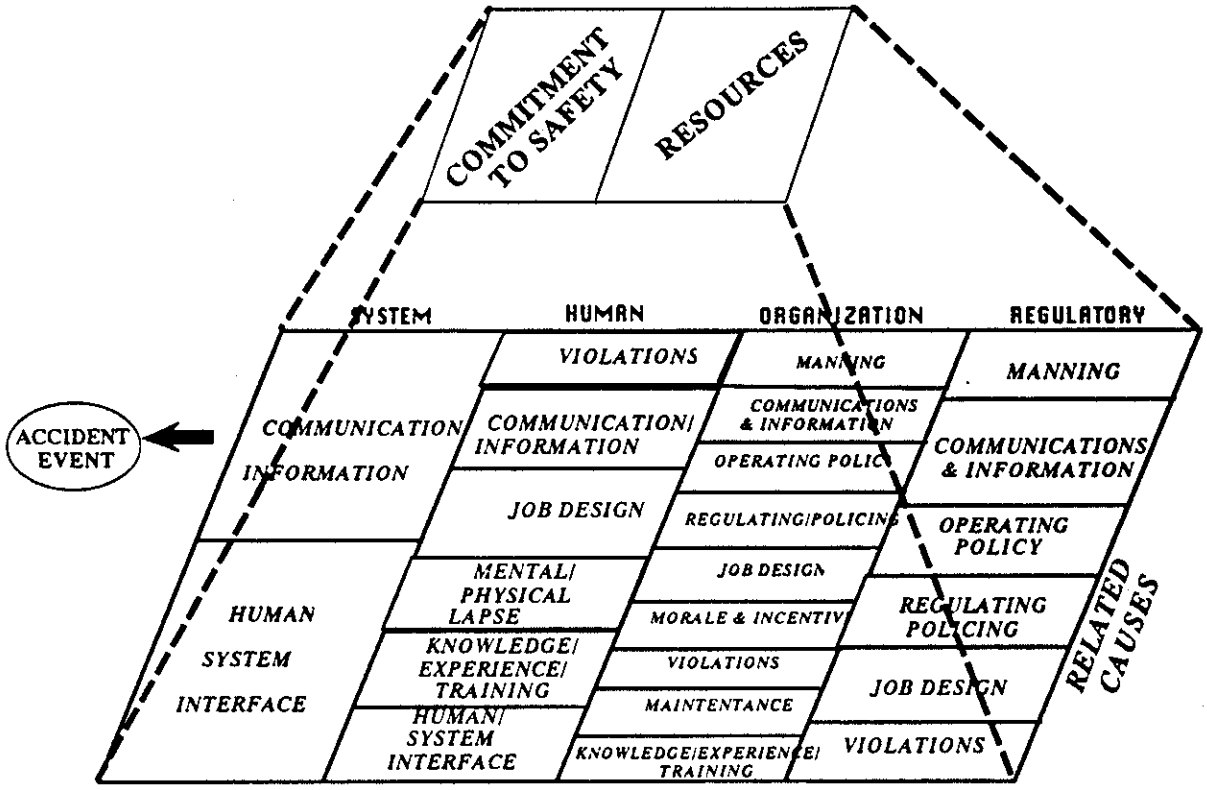


Fig. 1. Human and Organization Error Classification

PIPER ALPHA ANALYSIS

Fig. 2 is an influence diagram representation of the events, decisions and actions surrounding the *Piper Alpha* disaster. The night shift had just taken over operations onboard *Piper Alpha*.[4,5] The control room personnel were waking up and a contract maintenance crew had started maintenance work on one of the gas condensate pumps (Module C) that was not working properly (there were two of these pumps).

The production superintendent was assisting the maintenance crew in determining the source of the problem. Gas being produced from the platform and from two adjacent platforms and sent via pipeline to the platform, placed the platform on a code red status, indicating a maximum production situation. The production superintendent normally onboard the platform was on vacation. His position was filled by a replacement superintendent that had just come onboard the platform.

Earlier in the day, maintenance work had been partially completed on condensate pump B; it had been taken out of service to maintain its safety equipment, but the work was not completed before the night shift took over. The control room personnel were unaware of the maintenance work. Also, earlier in the day, divers had been in the water working on the underwater portions of the platform, and the fire pumps and deluge system (similar to a sprinkler system in a building) had been placed on manual control to prevent divers from being sucked into the sea water intakes.

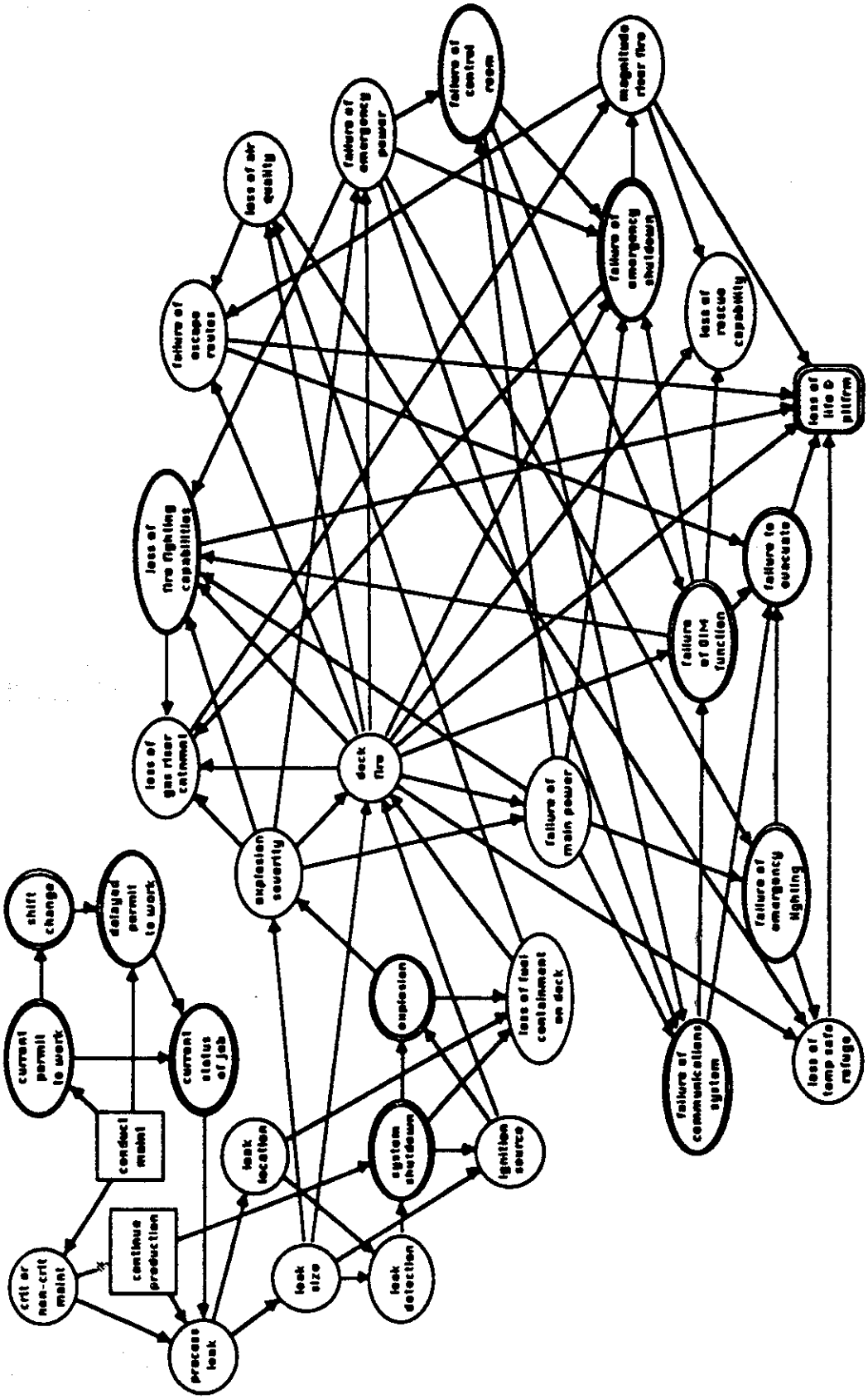


Fig. 2. Influence diagram representation of the Piper Alpha accident

The condensate pump B failed, and the order was given to the control room to turn on condensate pump A to avoid condensate from backing up into the gas compressors. The control room personnel did not realize that condensate pump A was not working and opened the valves to the pump, routing the gas condensate to the inoperable pump. Condensate and gas escaped into Module C and ignited causing an explosion, killing the crew and production superintendent. Due to the containment of the explosion, the adjacent control room was decimated. Power was lost due to destruction of the primary electrical wiring system by the explosion. The automatic deluge and emergency power systems did not come on because they had been placed on manual control and there was no one to manually activate the systems.

The fire quickly spread to adjacent oil and gas producing vessels and piping in Modules B and C. Unprotected fuel storage above the gas compression module was ignited and thick, dense, toxic smoke engulfed the quarters where surviving crew members were being mustered for evacuation in life boats. While awaiting the orders from the production superintendent to evacuate, fresh air intake fans sucked the smoke into the quarters. Because the production superintendent had been killed in the initial explosion, the evacuation orders never came, and in the dark and confusion the crew members were overcome by smoke and died.

Moored adjacent to the platform was an emergency support vessel. This vessel was designed specifically to provide emergency support to fight fires, kill well blowouts, accommodate divers and other field personnel, and provide emergency medical facilities. The vessel was instructed to fight fires at the order of the production superintendent. Again waiting for orders that could never come, and fearing for the safety of the vessel, the vessel master gave orders to pull back from the escalating fire. The fire fighting pumps were never used.

Pipelines bringing oil and gas from the *Tartan* and *Claymore* platforms passed immediately under the platform. Subjected to the intense heat, these lines softened and ruptured. A deafening explosion and fireball engulfed the entire platform. The emergency shut-in devices (to prevent the pipeline contents from escaping) were in the same area and were destroyed allowing the pipeline contents to be emptied into the fire. The result of these developments was total destruction of *Piper Alpha* and loss of 167 lives.

There were three primary stages in the accident sequence: (1) the decision to simultaneously conduct critical process maintenance and produce at a very high level, (2) the initial explosions and fires in Module C, and (3) the breach of fuel containment leading to additional fuel sources which escalated the fires to a level of catastrophic consequences resulting in the loss of lives and the platform. Fig. 3 illustrates the interactions of the HOE influences on the three primary stages in the accident. External environmental / operational conditions are indicated that influenced HOE.

HIGH PRESSURE GAS OPERATIONS INFLUENCE DIAGRAM

Based on the analysis of the *Piper Alpha* accident, a general template was developed for maintenance of a high pressure gas system involving simultaneous production operations (Fig. 4). The influence diagram focuses upon: (a) simultaneous production and maintenance leading to a gas leak, and (b) detection and control of the leak to prevent or mitigate fires or explosions leading to loss of fuel containment. Loss of fuel containment is assumed to result in large scal damage and consequence. The *Piper Alpha* disaster falls within this particular class of accidents.

The influence diagram identifies crew changes and communicating maintenance status. Distinctions are made between production and maintenance decisions. The maintenance location, duration, equipment, and reliability (abilities of maintenance crew) are included. To account for of maintenance operation, job duration and status, crew changes, communication of job status (permit to work system) directly or indirectly influence the magnitude of a process leak. Additional modifications account for production (maximum, moderate, or none) and process leak magnitudes (small, moderate, or large).

Fires and explosions are influenced by process leaks, leak location and type of production and maintenance. For example, concurrent high production and process critical maintenance greatly influence an explosion or fire event. The leak location and fire or explosion influence the loss of fuel containment (piping, fuel storage, risers, machinery and equipment). Human or system intervention are critical in detecting and gas leaks and ignition. System shutdown in the event of explosion or fire which can lead to failure of power and deluge systems. Breach of fire protection, production level, and failure of system shutdown lead to

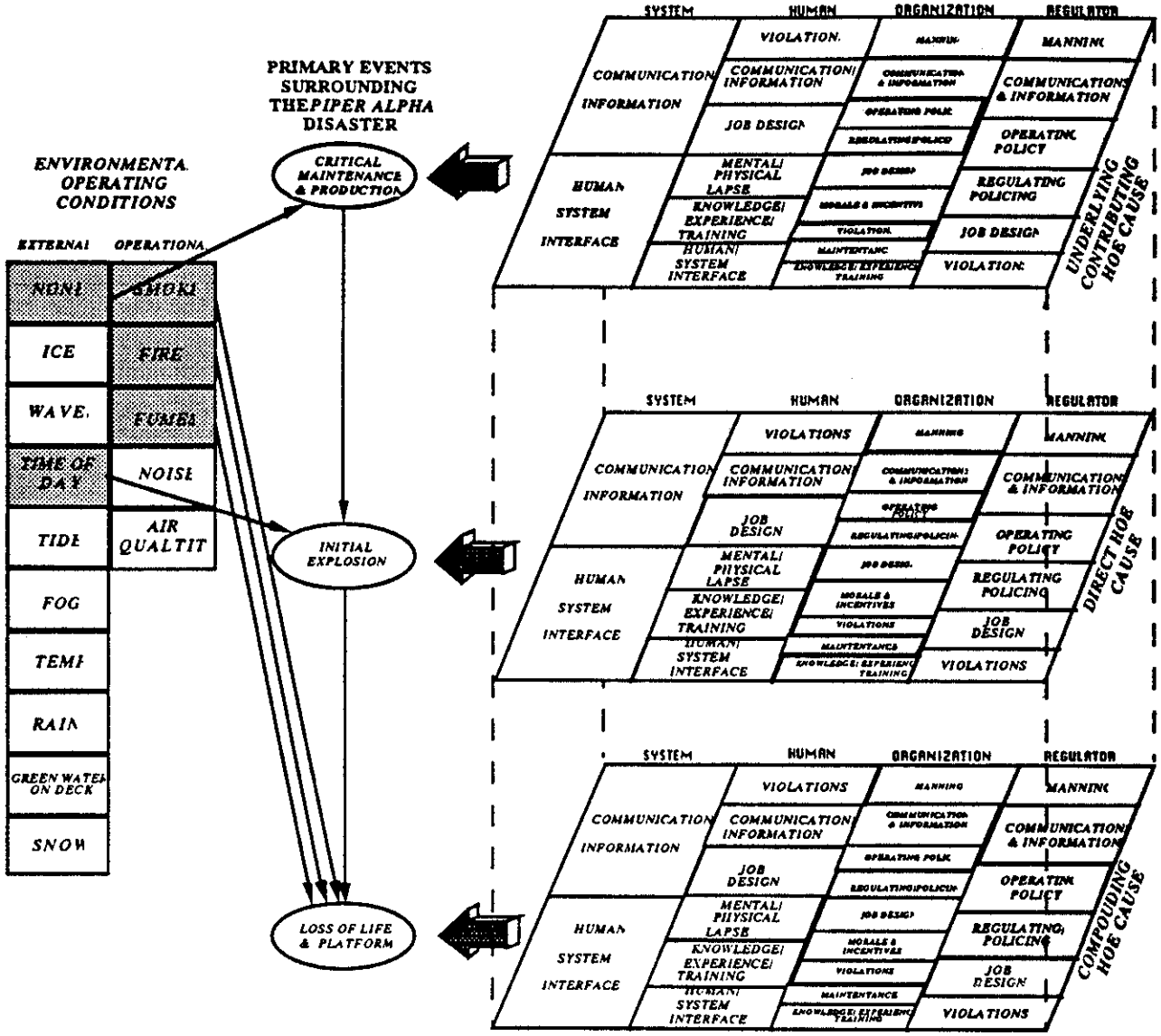


Fig. 3. HOE influences on the events of the *Piper Alpha* accident

the final failure event of loss of fuel containment.

Quantitative Assessments

Heuristic quantitative assessments were made to obtain probabilities of specified target events. The assessments were based on three levels of production (maximum, moderate, shut-down), four types of maintenance operations (process critical and non-critical and non-process critical and non-critical), the status of communications regarding the maintenance operations (status communicated or not communicated), the duration of the maintenance (less or greater than one shift), and the magnitude of the process leak (small, moderate, large). *Process critical maintenance* refers to maintenance on machinery and equipment directly related to producing and processing hydrocarbons (separators, compressors, risers, etc.). *Non-process critical maintenance* refers to maintenance that does not directly affect the production process (accommodations, utilities, structural, etc.).

The quantitative assessments were based on available accident data from sources including the U. S. Coast Guard CASMAIN database and the World Offshore Accident Database.[11] Due to the incompleteness and lack of sufficient definition in this data, the judgment and experience of operators, engineers, and managers

involved in these types of operations were utilized to encode the probabilities.

After reduction of the influence diagram shown in Fig. 4 conditional upon HOE factors, Table 1 summarizes the conditional probabilities of explosions or fires based upon the production/maintenance decisions. The explosion or fire is the particular initiating event to be avoided.

Explosions and fires are less frequent during non-process maintenance (approximately a factor of 2 for human errors and a factor of 3 for organizational and system errors). For human errors, the human/system interface has a higher frequency of accident occurrences. This may be attributed to problems in the control room as a result of sub-systems being shut down for maintenance or repair and system status information may be incomplete or incorrect. This is also evident with regard to system errors. Communications/ information and human system interface have comparatively higher frequencies of occurrence.

The loss of fuel containment is the compounding event to be avoided in wake of an explosion or fire. Table 2 summarizes: (1) the annual probabilities of explosions and fires conditional upon simultaneous production and maintenance schedules, (2) the annual probabilities of loss of fuel containment dependent upon explosions and fires and simultaneous production and maintenance schedules. The annual probabilities of loss of fuel containment are 2.5 times higher for producing and process critical maintenance operations than producing during non-process critical maintenance. The probabilities of loss of fuel containment in the event of explosion or fire are the same for both critical and non-critical maintenance operations.

Based on these evaluations and the influence diagram shown in Fig. 4, Table 3 summarizes the probabilities of getting a process leak onboard a platform configured and operated similar to *Piper Alpha* (refer to column P [leak] (prior). The likelihood of getting a large to moderate leak is approximately 10 % per year. The major contributor to this likelihood is the conduct of non-critical process maintenance whose status is not properly communicated and that takes more than one shift to complete. This is a direct "play-back" of the events that initiated the *Piper Alpha* accident. The other information in Table 3 will be discussed in the next section.

EVALUATION OF HOE MANAGEMENT ALTERNATIVES

Several alternatives for improved HOE management were assessed to determine how effective they might be at reducing the likelihood of a major accident. To illustrate the evaluation procedure, the *permit to work system* and *leak detection and control* were studied.

Permit to Work System (PWS)

In wake of the Lord Cullen Report,[4] the PWS for offshore maintenance operations has undergone a major re-evaluation and restructuring process. As mentioned previously, one of the primary contributors to the disaster was a process leak resulting from the lack of communication between maintenance crews and control room operators. In a study of U. K. platform safety, 76% of all accidents occurred during maintenance of which 30% of these accidents were failures in the PWS.[12]

The models were evaluated to determine the influences on process leak magnitudes using production levels, types of process maintenance (critical and non-critical), communicating maintenance status and duration as state variables.

As management alternatives, the PWS could be upgraded to provide better trained operators and maintenance crews, to computerize the PWS, and / or provide greater emphasis on detailed communication during crew changes. An enforced and verified discipline of communicating critical maintenance was the alternative investigated.

Similar PWS improvement programs in other industries (e.g. nuclear power, refineries) indicated an expected increase of maintenance status communication effectiveness by a factor of approximately 10. [13,14,15]

Table 3 tabulates the probabilities of process leaks before and after implementation of the improved PWS. The improved PWS program results in a reduction in the probability of all leaks by a factor of about 2 for maximum production levels during critical process maintenance. The improved PWS program results in a reduction in the probability of large leaks by a factor of 7 for all production levels. However, for maintenance during moderate production, little change in probability of leaks are indicated.

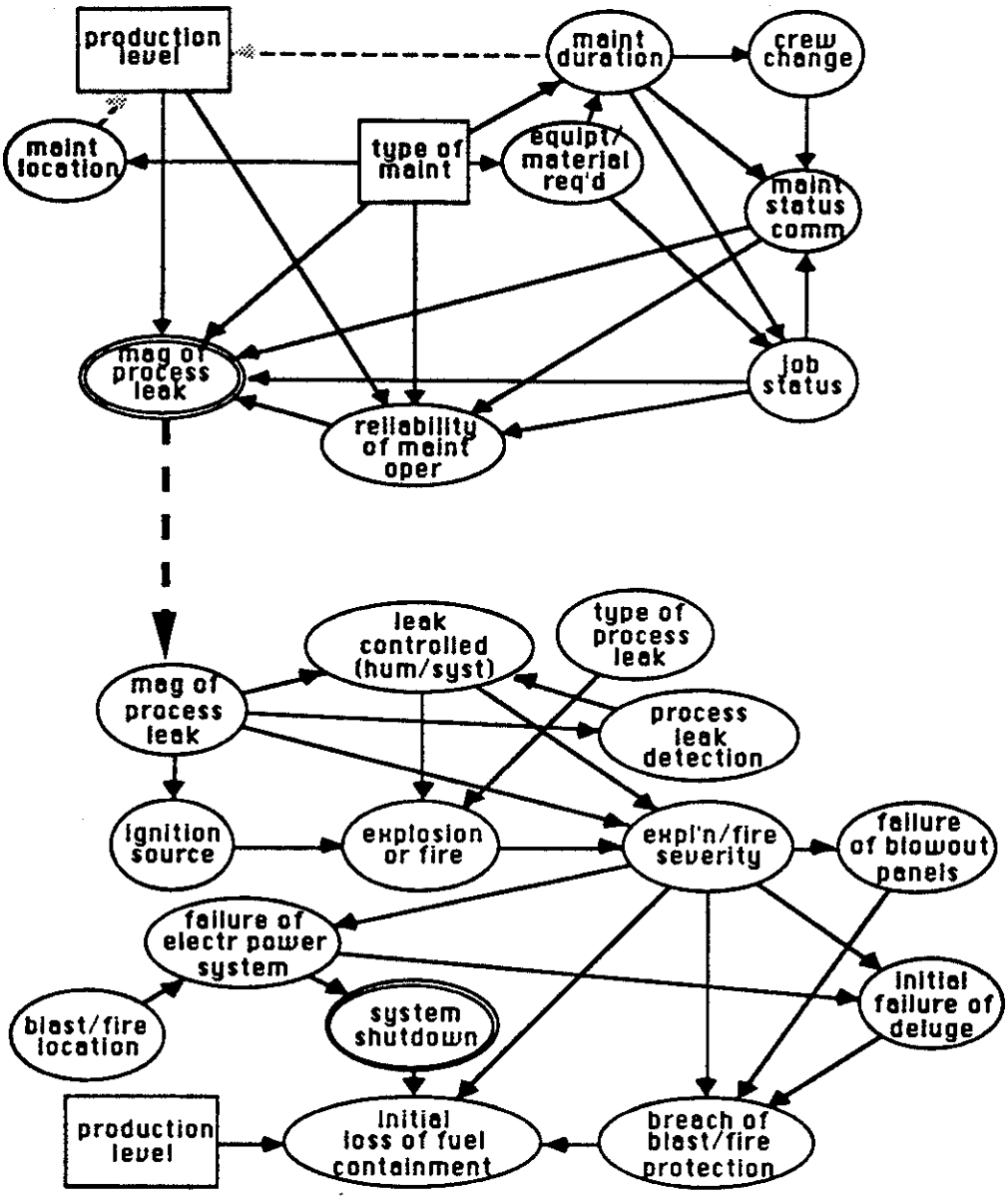


Fig 4. Influence diagram representation of simultaneous production and maintenance leading to process leak, explosion or fire, and loss of fuel containment

Process Leak Detection and Control (PLDC) System

PLDC can be performed both manually (operators) and automatically (system). The ability to detect and control process leaks are dependent upon the experience, knowledge and training of the operating crew, and the sensitivity of the detection and reliability of the control system.

Errors can be exacerbated by poorly engineered systems that invite errors. Such systems are difficult to construct, operate, and maintain.[16] New technologies can compound the problems of latent system flaws. Complex design, close coupling (failure of one component leads to failure of other components) and severe performance demands on systems increase the difficulty in controlling the impact of human errors even in well operated systems.[17] Emergency displays frequently have been found to give improper signals of the state of the systems.[4,17]

Human performance is a function of the lead time available to respond to warnings in the system. Errors are compounded by the lack of effective early warning systems.[18] If the lead time is short, there is little time allowance for corrective action before the situation reaches a critical state. On the other hand, if the system is too sensitive causing frequent false alarms, operators will eventually cease to respond to the warning signals.

If management invests in better training (crisis management), experience and knowledge (better incentives to qualified operators), detection (human-system interfacing, system communication and information) and emergency shutdown systems. These changes would result in better understanding of the process system and crisis management by front line operators.

An improved PLDC system was investigated that involved improvements in the physical leak detection system, in the emergency shut-down system, and in the fire suppression (deluge) system. Similar PLDC improvement measures have been implemented in other industries (e.g. nuclear power, refineries).[12,13,14]

The influence of the improved PLDC program influence the frequency of explosions or fires and are summarized in Table 4. The results indicate improved control and detection systems could be expected to lead to a decrease in the number of explosions and fires by a factor of 2.5. If not controlled, a reduction in the fire and explosions events for detected and uncontrolled leaks could be expected to be reduced by a factor of 2.

CONCLUSIONS

Post-mortem studies provide a basis in which to construct probabilistic models (influence diagrams) of general classes of accidents. Analyses of post-mortem accident studies lead to a greater understanding of the effects of HOE in accident sequences. Though quantitative data may be limited in availability and detail, using sound experience and judgment, engineers, managers and regulators are able to make reasonable evaluations of alternatives for managing HOE in operations of offshore production systems.

The results of the research project upon which this paper is based has indicated the following developments are needed to allow this approach to be integrated into engineering practice:

1) Further development and testing of a classification system for HOE, and

2) Further development of a human and organizational factor database management system to interface with the HOE analytical models.

Work on these topics is continuing.

ACKNOWLEDGMENTS

This paper is funded in part by a grant form the National Sea Grant College Program, National Oceanic and Atmospheric Administration, Department of Commerce, under grant number NA89AA-D-SG138, project number R/OE-17 through the California Sea Grant College, and in part by the California State Resources Agency. The views expressed herein are those of the authors and do not necessarily reflect the views of NOAA or any of its sub agencies. The U.S. Government is authorized to reproduce and distribute for government purposes.

This work also has been sponsored in part by Chevron Research & Technology Company and Chevron Shipping Company, Amoco Production Company and Amoco Transport Company, Unocal Corporation, the California State Lands Commission, the U.S. Coast Guard, the U.S. Minerals Management Service, and the American Bureau of Shipping. The support and guidance of these sponsors is gratefully acknowledged.

REFERENCES

[1] Bea, R.G. & Moore, W.H. "Management of Human and Organizational Error in Operational Reliability of Marine Structures," *Proceedings, Society of Naval Architects and Marine Engineers 2nd Offshore Symposium: Designs and Codes.* Houston, TX. April, 1991.

[2] Paté-Cornell, M.E. "A Post-Mortem Analysis of the *Piper Alpha* Accident: Technical and Organizational Factors," Research Report No. 92-2, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture*

and Offshore Engineering, University of California, Berkeley. September, 1992.

[3] Roberts K.H. & Moore W.H., "The Gordian Knot: Into Which Sailed the *Exxon Valdez*," Research Report No. 92-1, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering, University of California, Berkeley*. January, 1992.

[4] United Kingdom Department of Energy. *The Public Inquiry Into the Piper Alpha Disaster, The Hon Lord Cullen*, Volumes 1 & 2, HMSO Publications, London. November, 1990.

[5] Institute of Marine Engineers. "Offshore Operations Post *Piper Alpha*," Proceedings of the February 1991 Conference, London, England. 1991.

[6] Bea, R.G. & Moore, W.H. "Organizational Reliability and Marine Systems," *New Challenges to Understanding Organizations*, Macmillan: New York, 1993.

[7] Phillips, L. D., Humphreys, D. E., and Selby, D. L. "A Socio-Technical Approach to Assessing Human Reliability," From *Influence diagrams, belief nets and decision analysis*. Edited by Oliver, M.R. & Smith, J.Q. Wiley & Sons: New York. 1990.

[8] Howard, R.A. & Matheson, J.E. *Influence Diagrams*. Copyright © 1981.

[9] Howard, R.A. "From Influence to Relevance to Knowledge," From *Influence diagrams, belief nets and decision analysis*. Edited by Oliver, M.R. & Smith, J.Q. Wiley & Sons: New York. 1990.

[10] Moore, W.H. & Bea, R.G. "A Practical Human Error Taxonomy for Marine Related Casualties," Research Report No. 92-3, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering*, University of California, Berkeley. June, 1992.

[11] Moore, W.H. "Human and Organizational Error in Marine Systems: A Review of Existing Taxonomies and Databases," Research Report No. 91-1, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering*, University of California at Berkeley. July, 1991.

[12] Lee, B.S. & McMillan, W.S. "A Knowledge Based System for Offshore Permit to Work Management," *Proc. of Second International Offshore and Polar Engineering Conference*. 1992.

[13] Bell, B. J. & Swain, A. D. *A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants*, Div. of Facility Operations, Office of Nuclear Regulatory Research, U. S. Nuclear Regulatory Commission, Report NUREG/CR-2254, Washington, D. C. 1981.

[14] Swain, A. D., and Guttmann, H. E. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, Office of Nuclear Regulatory Research, U. S. Nuclear Regulatory Commission, Report NUREG/CR-1278, Washington, D. C. 1983.

[15] Swain, A. D. *Safety Analysis and Risk Assessment for Chemical Process Industry Practitioners: Human Reliability Analysis*, American Institute of Chemical Engineers, New Jersey, Oct., 1988.

[16] Melchers, R.E. *Structural Reliability Analysis and Prediction*. Brisbane, Australia: Ellis Horwood Limited, Halsted Press: a division of John Wiley & Sons, 1987.

[17] Perrow, C. *Normal Accidents: Living with High Risk Technologies*. New York: Basic Books, Inc., 1984.

[18] Paté-Cornell, M. E. "Warning Systems in Risk Management," *Risk Analysis*, Vol. 6, No.2. 1986.

Table 1
Conditional probabilities of explosions and fires based upon production and maintenance operations

	Probability [explosion/fire] error]/yr	
	proc critical maint & production	non-proc maint & production
Human errors		
none	2.2E-5 / 2.2E-5	9.0E-6 / 9.0E-6
violations	4.4E-5 / 4.4E-5	2.1E-5 / 2.1E-5
comm/info	4.4E-5 / 4.4E-5	2.4E-5 / 2.4E-5
job design	4.4E-5 / 4.4E-5	2.4E-5 / 2.4E-5
mntl/phys lapse	4.4E-5 / 4.4E-5	2.1E-5 / 2.1E-5
knwl/expr/trng	4.4E-5 / 4.4E-5	2.1E-5 / 2.1E-5
hum/syst intrfc	1.65E-4 / 1.65E-4	4.8E-5 / 4.8E-5
Organizational/management errors		
none	2.4E-5 / 2.4E-5	9.0E-6 / 9.0E-6
manning	2.9E-5 / 2.9E-5	1.3E-5 / 1.3E-5
comm/info	3.5E-5 / 3.5E-5	1.3E-5 / 1.3E-5
oper policy	2.8E-5 / 2.8E-5	1.2E-5 / 1.2E-5
regul/policing	2.8E-5 / 2.8E-5	1.2E-5 / 1.2E-5
job design	3.1E-5 / 3.1E-5	1.2E-5 / 1.2E-5
moral/incent	2.9E-5 / 2.9E-5	1.2E-5 / 1.2E-5
violations	2.9E-5 / 2.9E-5	1.3E-5 / 1.3E-5
maintenance	2.8E-5 / 2.8E-5	1.1E-5 / 1.1E-5
knwl/exp/trning	2.6E-5 / 2.6E-5	1.3E-5 / 1.3E-5
System errors		
none	2.5E-5 / 2.5E-5	1.0E-5 / 1.0E-5
comm/info	3.7E-5 / 3.7E-5	1.3E-5 / 1.3E-5
hmn syst intrface	4.3E-5 / 4.3E-5	1.4E-5 / 1.4E-5

Table 2
Conditional probabilities of explosions and fires based upon production and maintenance operations

	proc critical maint & production	non-proc maint & production
Probability [explosion/fire] maintenance schedule]/yr	2.5E-5 / 2.5E-5	1.0E-5 / 1.0E-5
Probability [loss of fuel containment | maintenance schedule & explosion or fire]/yr		
Fire	0.098956	0.114853
Explosion	0.115440	0.119265

Table 3
Conditional probabilities of process leaks per year

production level	type of maint	status of maint	duration of maint	process leak magnitude	P[leak] (prior)	P[leak] (post)
maximum	process critical	communic status	less than a shift	sm leak mod leak lg leak	0.075 0.0012 1.9E-5	0.038 8.0E-4 4.4E-6
"	"	"	greater than a shift	sm leak mod leak lg leak	0.096 1.8E-4 1.3E-4	0.048 1.7E-4 1.8E-5
"	"	status not communic	"	sm leak mod leak lg leak	0.21 0.043 .0029	0.15 0.0066 0.0020
"	process non-critical	communic stautus	less than a shift	sm leak mod leak lg leak	0.021 0.011 0.0034	0.0034 0.004 0.001
"	"	"	greater than a shift	sm leak mod leak lg leak	.04 3.0E-4 1.6E-4	.007 1.2E-4 3.0E-5
"	"	status not communic	"	sm leak mod leak lg leak	.17 0.0060 .0041	0.11 9.0E-4 3.5E-4
"	non-process critical	communic status	less than a shift	sm leak mod leak lg leak	6.3E-4 0.0 0.0	6.04E-4 0.0 0.0
"	"	"	greater than a shift	sm leak mod leak lg leak	6.3E-4 0.0 0.0	6.04E-4 0.0 0.0
"	"	status not communic	"	sm leak mod leak lg leak	6.3E-4 0.0 0.0	6.04E-4 0.0 0.0
"	non-process non-crit	communic status	less than a shift	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
"	"	"	greater than a shift	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
"	"	status not communic	"	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
moderate	process critical	status commun	less than a shift	sm leak mod leak lg leak	0.0075 0.0013 0.0	0.0075 0.0013 0.0
"	"	"	greater than a shift	sm leak mod leak lg leak	0.0096 1.8E-5 0.0	0.0039 1.7E-5 0.0
"	"	status not communic	"	sm leak mod leak lg leak	0.0095 0.02 5.0E-4	0.0043 0.005 5.0E-4
"	process non-crit	status communic	less than a shift	sm leak mod leak lg leak	.0019 .006 .004	.0002 4.0E-4 6.1E-5

Table 3
Conditional probabilities of process leaks per year (continued)

production level	type of maint	status of maint	duration of maint	process leak magnitude	P[leak] (prior)	P[leak] (post)
moderate	process non-crit	status communic	greater than a shift	sm leak mod leak lg leak	2.7E-4 0.0 0.0	2.7E-4 0.0 0.0
"	"	status not communic	"	sm leak mod leak lg leak	6.3E-4 0.0 0.0	6.0E-4 0.0 0.0
"	non-process critical	status communic	less than a shift	sm leak mod leak lg leak	0.005 5.0E-4 0.0	8.0E-4 5.0E-5 0.0
"	"	"	greater than a shift	sm leak mod leak lg leak	0.0092 7.8E-4 0.0	0.0013 1.3E-4 0.0
"	"	stuatus not communic	"	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
"	non-process non-crit	communic stauts	less than a shift	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
"	"	"	greater than a shift	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
"	"	status not communic	"	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
none	no leaks	no leaks	no leaks	no leaks	0.0	0.0

Table 4

Probabilities of explosion or fire with and without an improved PLDC system

leak control	process leak detection	explosion or fire	P[explosion or fire] (prior)	P[explosion or fire] (post)
leak control	detected	fire	0.0075	0.0020
"	"	explosion	0.0075	0.0020
no leak control	"	fire	0.21	0.10
"	"	explosion	0.21	0.11
"	not detected	fire	0.44	0.44
"	"	explosion	0.44	0.44

Presentation paper for the American Society of Mechanical Engineers
OFFSHORE MECHANICS AND ARCTIC ENGINEERING CONFERENCE
Glascow, Scotland June, 1993

HUMAN AND ORGANIZATIONAL ERROR IN OPERATIONS OF MARINE SYSTEMS: OCCIDENTAL *PIPER ALPHA*

William H. Moore
Department of Naval Architecture & Offshore Engineering
University of California
Berkeley, California

Robert G. Bea
Department of Naval Architecture & Offshore Engineering
and Department of Civil Engineering
University of California
Berkeley, California

ABSTRACT

Based on the well-documented case history of the Piper Alpha *catastrophe, probability based influence diagrams have been developed for the direct and compounding sequences of events that led up to the initial explosion. This analysis structure has been used to develop a simplified general "template" for high pressure gas operations that preserves the central causative mechanisms, yet does not preserve the unique aspects of the* Piper Alpha *disaster. This template is used to examine the potential influences of alternative improvements in operations intended to reduce the potential for HOE.*

INTRODUCTION

This paper summarizes the results from a post mortem study of the Occidental *Piper Alpha* disaster which led to the death of 167 men and total loss of platform. The roots of this accident are firmly founded in compounded human (onboard operating personnel) and organizational (Occidental Petroleum, Department of Energy) errors (HOE). In the aftermath of the events, much effort has focused on technical and systemic fixes with little effort spent on the HOE aspects.

As part of a long-term research program to improve the reliability of marine systems being conducted at the University of California, the roles of HOE in operations of marine systems have been examined. This study has resulted in development of a classification of such errors to help understand and evaluate the roles of HOE. The qualitative and quantitative characterizations developed in the analyses are based on an extensive study of well-documented case histories and databases of catastrophic marine casualties. Available accident data are severely deficient in properly recognizing and recording HOE aspects of prior accidents. This places a heavy burden on appropriate experience based judgment to properly interpret available casualty statistics in relation to the roles of HOE in these catastrophes.

BACKGROUND

Approximately 65% of catastrophic marine accidents are the result of compounded human and organizational errors (HOE) during operations. Yet to date there is no structured quantitative approach to assist engineers, operators, and regulators of marine systems to design human and organizational error (HOE) tolerant systems. No considerations have been established to include HOE as an integral part of the design, construction, and operation of offshore structures (Bea and Moore, 1991).

This understanding has led to a Joint Industry Project entitled *Management of Human Error in Operations of Marine Systems*. The purpose of the project is to: (1) develop an organization and classification of the sources of the errors, (2) determine how the errors interact to cause the accidents, (3) investigate the effectiveness of various alternatives in reducing HOE in operations of tankers and offshore platforms, and (4) evaluate the tradeoffs between the costs and benefits (risk reduction) of alternative HOE control strategies.

An error classification has been developed to use in the analysis framework and is used for categorizing and describing HOE in the accident model (Figure 1) (Moore and Bea, 1992). Detailed analytical case studies were developed from the *Piper Alpha* and the *Exxon Valdez* disasters during this project. These case studies were used to establish a qualitative framework to examine the primary HOE and technological contributions to the accidents (Paté-Cornell, 1992; Roberts and Moore, 1992).

The *Piper Alpha* disaster was selected as a case history based upon the quality, completeness, accessibility, and availability of information related to the accident events.

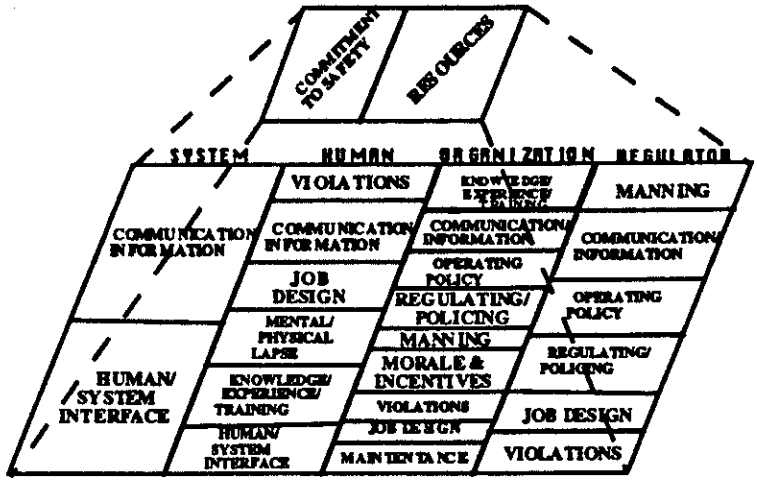


Figure 1: Human and organizational error classification for marine casualties

The report by Paté-Cornell (1992) on the *Piper Alpha* disaster and the HOE error classification developed by Moore and Bea (1992) form the basis from which the model in this paper was developed.

PIPER ALPHA ACCIDENT EVENTS

The night shift had just taken over operations onboard *Piper Alpha*. The control room personnel were waking up and a contract maintenance crew had started maintenance work on one of the gas condensate pumps (Module C) that was not working properly (there were two of these pumps).

The production superintendent was assisting the maintenance crew in determining the source of the problem. Gas was produced from two adjacent platforms and was sent via pipeline to *Piper Alpha*. This operational combination placed *Piper Alpha* on a code red status, indicating a maximum production situation. The production superintendent normally onboard the platform was on vacation. His position was filled by a replacement superintendent who had just come onboard the platform.

Earlier in the day, maintenance work had been partially completed on condensate pump B; it had been taken out of service, however, the work had not completed before the night shift took over. The control room personnel were unaware of the maintenance work. Also, earlier in the day, divers had been in the water working on the underwater portions of the platform, and the fire pumps and deluge system (similar to a sprinkler system in a building) had been placed on manual control to prevent divers from being sucked into the sea water intakes.

The condensate pump B failed, and the order was given to the control room to turn on condensate pump A to avoid condensate from backing up into the gas compressors. The control room personnel did not realize that condensate pump A was not working and opened the valves to the pump, routing the gas condensate to the inoperable pump. Condensate and gas escaped into Module C and ignited causing an explosion, killing the crew and production superintendent. Due to the containment of the explosion, the adjacent control room was decimated. Power was lost due to destruction of the primary electrical wiring system by the explosion. The automatic deluge and emergency power systems did not respond because they had been placed on manual control There was no one to manually activate the systems.

The fire quickly spread to adjacent oil and gas producing vessels and piping in Modules B and C. Unprotected fuel storage above the gas compression module was ignited and thick, dense, toxic smoke engulfed the quarters where surviving crew members were being mustered for evacuation in life boats. While awaiting the orders from the production superintendent to evacuate, fresh air intake fans sucked the smoke into the quarters. Because the production superintendent had been killed in the initial explosion, the evacuation orders never came, and in the dark and confusion the crew members were overcome by smoke and died.

Moored adjacent to the platform was the emergency support vessel, *M.S. Tharos*. This vessel was designed specifically to provide emergency support to fight fires, kill well blowouts, accommodate divers and other field personnel, and provide emergency medical facilities. The vessel was instructed to fight fires at the order of the production superintendent. Again waiting for orders that could never come, and fearing for the safety of the vessel, the vessel master gave orders to pull back from the escalating fire. The fire fighting pumps were never used.

Pipelines bringing oil and gas from the *Tartan* and *Claymore*

platforms passed immediately under the platform. Subjected to the intense heat, these lines softened and ruptured. A deafening explosion and fireball engulfed the entire platform. The emergency shut-in devices (to prevent the pipeline contents from escaping) were in the same area and were destroyed allowing the pipeline contents to be emptied into the fire. The result of these developments was total destruction of *Piper Alpha* and loss of 167 lives.

ACCIDENT FRAMEWORK MODELS

Four principal steps are involved in the developments of a post-mortem study analysis: (1) structuring the relevant events, decisions, and actions specific to the accident scenario, (2) applying human and organizational error classifications to identify contributing factors, and (3) development of model classification frameworks in which the accident falls within that class, and (4) determine a general set of contributing HOE causes related to events, decisions, and actions for the particular class of accidents.

Models Representing Classes of Accidents

The intent is to develop (and verify) PRA models to include the reliability effects of human and organizational factors. The general method is to integrate elements of process analysis and organizational analysis in assessing the probability of system failure (Paté-Cornell and Bea, 1989; Paté-Cornell and Seawell, 1988). The first phase is a preliminary *probabilistic risk analysis* (PRA) to identify the key subsystems or elements of the system's reliability. The second phase is an analysis of the process to identify potential problems within each subsystem and their probabilities or base rates per time unit or per operation.

Given that a basic error occurs, analysis of the organizational procedures and incentive system is performed to determine their influence on the occurrence of basic errors and the probability that they are observed, recognized, communicated, and corrected in time (i.e. before a system failure event). The risk analysis model includes relevant decisions, actions and organizational features in the risk assessment and management. This procedure requires the user to establish an exhaustive set of contributing events and determine relevant decisions and actions specific to the class of accidents of interest (explosions, fires, groundings, collisions, etc.).

A probabilistic model of the process includes determining the set of possible initiating accident events (in_i) and final states ($fist_m$) of the system. The probability of loss of components (platform, vessel, revenue, life, injury, etc.) to the system can then be represented by:

$$p(loss_k) = \sum_i \sum_m p(in_i)\, p(fist_m | in_i)\, p(loss_k | fist_m) \qquad \forall\, k. \qquad (1)$$

The model is expanded to include relevant decisions and actions (A_n) constituting an exhaustive and mutually exclusive set of decisions or actions affecting the system at different stages during the lifetime of the platform. These decisions and actions can be examined from the level of front-line operating crew through top-level management.

$$p(loss_k) = \sum_i \sum_m \sum_n p(A_n)\, p(in_i | A_n)\, p(fist_m | in_i, A_n)\, p(loss_k | fist_m, A_n) \qquad \forall\, k. \qquad (2)$$

The effects of organizational procedures and policies on operational risks are determined through examining the probabilities of actions and decisions conditional on relevant organizational factors (O_h). The probabilities of various degrees of loss can be examined conditional upon different contributing organizational factors. Further developments into the quantitative aspects of HOE is the subject of a future report.

$$p(loss_k | O_h) = \sum_i \sum_m \sum_n p(A_n | O_h)\, p(in_i | A_n)\, p(fist_m | in_i, A_n)\, p(loss_k | fist_m, A_n) \qquad (3)$$

Influence Diagrams

Accident framework models for PRA analysis are constructed using *influence diagrams*. Influence diagramming allows greater flexibility in examining HOE and HOE management alternatives. Influence diagrams are an alternative to standard event/fault tree analyses to assess conditional probabilities required for determining unconditional probabilities of specified target events (Phillips, *et al.*, 1988).

As described by Howard (1990), the components of an influence diagram are: (1) *decision* and *chance nodes*, (2) *arrows*, (3) *deterministic nodes*, and (4) *value nodes* (Howard, 1990). Decisions are represented by square nodes which can be a continuous or discrete variable or set of decision alternatives (see Figure 4). Uncertain events or variables are represented by circular or oval chance nodes. Chance nodes are continuous or discrete random variables or a set of events. Arrows indicate relationships between nodes in the diagram. Arrows entering a chance node represent the probability assignments of the node are conditional from where the arrow originated. Deterministic nodes depend deterministically upon its predecessors. A value node is designated as: "the quantity whose certain equivalent is to be optimized by the decisions". Only one node may be designated in the diagram and is represented by a rounded edge double-border rectangle.

Structuring Events, Decisions, and Actions

To establish the accident events, decisions, actions, and causes, a preliminary diagram representation of the accident can be constructed. The diagram is not an influence diagram per se since no probabilities are assessed, but a representation of the accident factors which occurred. The purpose of the diagram is to assist the user in establishing the relevant contributing factors unique to the specific accident sequence. Figure 2 is a model of specific factors which led to the loss of fuel containment aboard *Piper Alpha*. The preliminary diagram assists the user in identifying critical areas where:

(1) risk and consequences may be managed and controlled, or
(2) further detailed study may be warranted.

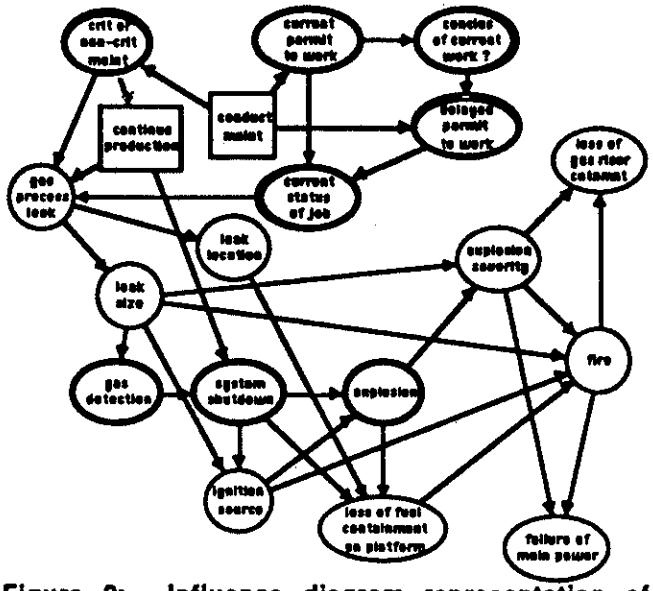


Figure 2: Influence diagram representation of primary contributors to the *Piper Alpha* disaster

The analysis structure has been used to develop a simplified and generalized "template" for high pressure gas operations that preserves the central causative mechanisms and not the unique aspects of the *Piper Alpha* disaster. The model development (and preliminary model representations) is generally the result of the efforts of a group of experts. Discussion of differences in opinion of relationships between events and their causes illicit the development of more realistic models (Phillips, *et al.*, 1990).

The modeling process includes the structuring of a target event which is the final result of contributing events, decisions, and actions (e.g. platform fire, loss of life or platform, etc.) (Paté-Cornell, 1992). The first step is to establish dependencies between relevant events decisions and actions which are categorized into three states:

(1) *Contributing/underlying events, decisions and actions*: Contributing/ underlying events are those occurring prior to the initiating accident event contributing to the reduction of reliability or increase of risk for the system (decision to simultaneously produce and conduct process maintenance on *Piper Alpha*).

(2) *Initiating/direct accident events, decisions, and actions*: The immediate accident event(s), decisions, and actions resulting in the casualty (the initial explosions and fires were the result of unfinished maintenance of condensate pumps in Module C).

(3) *Compounding events, decisions and actions*: The events, decisions, and actions lead to compounding of accident consequences (increasing the flow of gas to *Piper Alpha* from satellite platforms *Claymore* and *Tartan*).

As shown in Figure 3, the impact of HOE's are examined based upon the primary events, decisions, and actions, of the operation (Bea and Moore, 1992). Environmental conditions (temperature, waves, smoke, fire, etc.) influenced events, decisions, actions and HOE's and are incorporated into the model.

HIGH PRESSURE GAS SYSTEM TEMPLATE

The influence diagram template for high pressure gas systems shown in Figure 4 directly focus upon (1) simultaneous production and maintenance leading to a gas leak, and (2) detection and control of the leak to prevent or mitigate fires or explosions. The final consequence is a loss of fuel containment. The *Piper Alpha* disaster falls within this particular class of accidents.

The influence diagram models crew changes and communicating maintenance status. Distinctions are made between production and maintenance decisions. The maintenance location, duration, equipment, and reliability (abilities of maintenance crew) are included. To account for maintenance operation, job duration and status, crew changes, communication of job status (permit to work system) directly or indirectly influence the size of a process leak. Additional modifications account for production (maximum, moderate, or none) and process leak size (small, moderate, or large).

Fires and explosions are influenced by process leak, leak location, and type of production and maintenance. For example, concurrent high production and process critical maintenance greatly influence an explosion or fire event. The leak location and fire or explosion influence loss of fuel containment (piping, fuel storage, risers, machinery and equipment). Human or system intervention are critical in detecting and gas leaks and ignition. Emergency systems shutdown in the event of explosion or fire possibly leading to failure of power and deluge systems. Breach of fire protection, production level, and failure of system shutdown lead to a final failure event of loss of fuel containment.

Quantitative Assessments

Heuristic quantitative assessments were made to obtain probabilities of specified target events. The assessments were based on three levels of production (maximum, moderate, and shut-down), four types of maintenance operations (process critical or non-critical, and non-process critical or non-critical), the status of communications regarding the maintenance operations (status communicated or not communicated), the duration of the maintenance (greater or less than a work shift), and process leak size (small, moderate, or

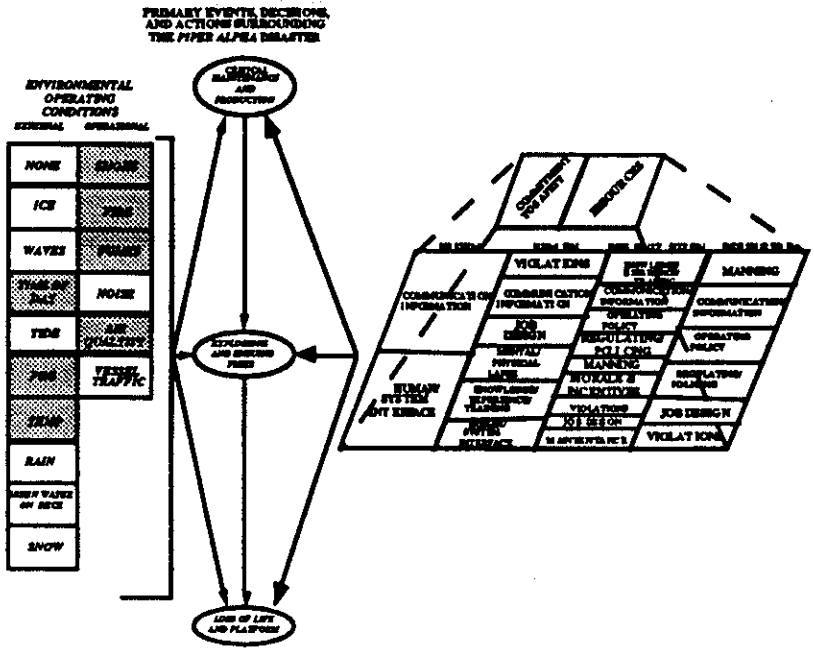


Figure 3: HOE and environmental influences on primary events surrounding the *Piper Alpha* disaster

large). *Process critical maintenance* refers to maintenance on machinery and equipment directly related to producing and processing hydrocarbons (separators, compressors, risers, etc.). *Non-process critical maintenance* refers to maintenance that does not directly affect the production process (accommodations, utilities, structural, etc.).

The quantitative assessments were based upon available accident data from sources including the U.S. Coast Guard CASMAIN database and the World Offshore Accident Database. Due to the incompleteness and lack of sufficient definition in this data, the judgment and experience of operators, engineers, and managers involved in these types of operations were utilized to encode the probabilities.

After reduction of the influence diagram shown in Figure 4 conditional upon HOE factors, Table 1 summarizes the conditional probabilities of explosions or fires based upon the production/maintenance decisions. The explosion or fire is the particular initiating event to be avoided.

Explosions and fires are less frequent during non-process maintenance (approximately a factor of 2 for human errors and a factor of 3 for organizational and system errors). For human errors, the human/system interface has a higher frequency of accident occurrences. This may be attributed to problems in the control room as a result of sub-systems being shut down for maintenance or repair. The status of the system may be incomplete or incorrect. Communications/ information and human system interface are assumed to have comparatively higher frequencies of occurrence.

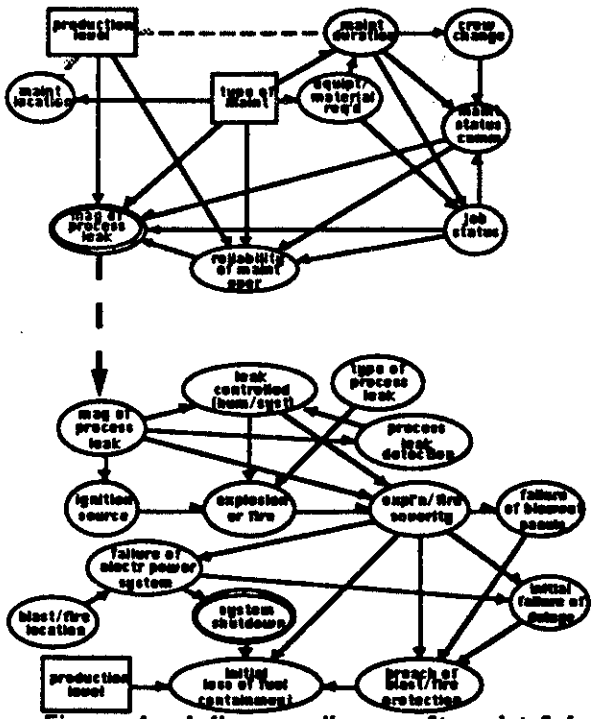


Figure 4: Influence diagram "template" for high pressure gas systems

Table 1
Probability of explosions or fires conditional upon production / maintenance operations

	Probability [explosion/fire/ error]/yr	
	proc critical maint & production	non-proc maint & production
Human errors		
none	2.2E-5 / 2.2E-5	9.0E-6 / 9.0E-6
violations	4.4E-5 / 4.4E-5	2.1E-5 / 2.1E-5
comm/info	4.4E-5 / 4.4E-5	2.4E-5 / 2.4E-5
job design	4.4E-5 / 4.4E-5	2.4E-5 / 2.4E-5
mntl/phys lapse	4.4E-5 / 4.4E-5	2.1E-5 / 2.1E-5
knwl/exp/trng	4.4E-5 / 4.4E-5	2.1E-5 / 2.1E-5
hum/syst intrfc	1.7E-4 / 1.7E-4	4.8E-5 / 4.8E-5
Organizational/ management errors		
none	2.4E-5 / 2.4E-5	9.0E-6 / 9.0E-6
manning	2.9E-5 / 2.9E-5	1.3E-5 / 1.3E-5
comm/info	3.5E-5 / 3.5E-5	1.3E-5 / 1.3E-5
oper policy	2.8E-5 / 2.8E-5	1.2E-5 / 1.2E-5
regul/policing	2.8E-5 / 2.8E-5	1.2E-5 / 1.2E-5
job design	3.1E-5 / 3.1E-5	1.2E-5 / 1.2E-5
moral/incent	2.9E-5 / 2.9E-5	1.2E-5 / 1.2E-5
violations	2.9E-5 / 2.9E-5	1.3E-5 / 1.3E-5
maintenance	2.8E-5 / 2.8E-5	1.1E-5 / 1.1E-5
knwl/exp/trning	2.6E-5 / 2.6E-5	1.3E-5 / 1.3E-5
System errors		
none	2.5E-5 / 2.5E-5	1.0E-5 / 1.0E-5
comm/info	3.7E-5 / 3.7E-5	1.3E-5 / 1.3E-5
hmn syst intrface	4.3E-5 / 4.3E-5	1.4E-5 / 1.4E-5

The loss of fuel containment is the compounding event to be avoided in wake of an explosion or fire. Table 2 summarizes: (1) the annual probabilities of explosions and fires conditional upon simultaneous production and maintenance schedules, (2) the annual probabilities of losing fuel containment depend upon explosions and fires and simultaneous production and maintenance schedules. The annual probabilities of loss of fuel containment are 2.5 more frequent for producing and process critical maintenance operations than producing during non-process critical maintenance. The probabilities of loss of fuel containment in the event of explosion or fire are the same for both critical and non-critical maintenance operations.

Table 2
Probabilities of explosions or fires conditional upon production and maintenance operations

Probability [explosion/fire/ maintenance schedule]/yr	
2.5E-5 / 2.5E-5 (process crit)	1.0E-5 / 1.0E-5 (non-process crit)
Probability [loss of fuel containment / maintenance schedule & explosion or fire]/yr	
Fire	0.099956 (process crit) 0.114853 (non-process crit)
Explosion	0.11544 (process crit) 0.119265 (non-process crit)

Based on these evaluations and influence diagram shown in Figure 4, Table 3 summarizes the probabilities of having a process leak onboard a platform configured and operated similar to *Piper Alpha* (refer to column P[leak] (prior)). The likelihood of having a large or moderate leak is approximately 10% per year. The major contributor to this likelihood is conducting of non-critical process maintenance whose status is not properly communicated, and taking more than a single work shift to complete. This is a direct "playback" of the events that initiated the *Piper Alpha* accident.

EVALUATION OF HOE MANAGEMENT ALTERNATIVES

Several alternatives for improved HOE management were assessed to determine how effective they might be at reducing the likelihood of a major accident. To illustrate the evaluation procedure, the *permit to work system* and *leak detection and control system* were examined.

Permit to Work System (PWS)

In wake of the Lord Cullen Report (1990), the PWS for offshore maintenance operations has undergone a reevaluation and restructuring process worldwide. As mentioned previously, one of the primary contributors to the disaster was a process leak resulting from communication errors between maintenance crews and control room operators. In a study of U. K. platform safety, 76% of all accidents occurred during maintenance of which 30% of these accidents were failures in the PWS (Lee and McMillan, 1992).

The models were evaluated to determine the influences of HOE on process leak sizes for production levels, types of process maintenance (critical and non-critical), maintenance status communication and duration as state variables.

As management alternatives, the PWS could be upgraded to provide highly trained operators and maintenance crews, to computerize the PWS, and / or provide greater emphasis on better communication during crew changes. Verifying and enforcing proper communication during critical maintenance was the alternative investigated.

Similar to PWS improvement programs in other industries (e.g. nuclear power, refineries) communication effectiveness is expected to increase by a factor of approximately 10 (Bell and Swain, 1981; Swain and Guttmann, 1983; Swain, 1988).

Table 3 is a tabulation of the probabilities of process leaks before and after implementation of the improved PWS. The improved PWS program results in a reduction in the probability of all leaks by a factor of about 2 for maximum production levels for critical process maintenance. The improved PWS program results in a reduction in the probability of large leaks by a factor of 7 for all production levels. However, for maintenance during moderate production, little change in probability of leaks was observed.

Table 3
Conditional probabilities of process leaks

produce level	type of maint	status of maint	duration of maint	process leak mag	P[leak] (prior)	P[leak] (post)
maximum	process critical	commun status	less than a shift	sm leak mod leak lg leak	0.075 0.0012 1.86E-5	0.0375 8.0E-4 4.44E-6
"	"	"	greater than a shift	sm leak mod leak lg leak	0.096486 1.76E-4 1.32E-4	0.04832 1.68E-4 1.76E-5
"	"	status not commun	"	sm leak mod leak lg leak	0.20823 0.09277 .002939	0.15 0.06552 0.00022
"	process non-critical	commun status	less than a shift	sm leak mod leak lg leak	0.0208 0.011 0.0034	0.0034 0.004 0.001
"	"	"	greater than a shift	sm leak mod leak lg leak	.04 3.0E-4 1.61E-4	.007 1.2E-4 3.0E-5
"	"	status not commun	"	sm leak mod leak lg leak	.17 0.06007 .04112	0.11038 .009 .00346
"	non-process critical	commun status	less than a shift	sm leak mod leak lg leak	5.3E-4 0.0 0.0	5.04E-4 0.0 0.0
"	"	"	greater than a shift	sm leak mod leak lg leak	5.3E-4 0.0 0.0	5.04E-4 0.0 0.0
"	"	status not commun	"	sm leak mod leak lg leak	5.3E-4 0.0 0.0	5.04E-4 0.0 0.0
"	non-process non-crit.	commun status	less than a shift	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
"	"	"	greater than a shift	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
"	"	status not commun	"	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
moderate	process critical	status commun	less than a shift	sm leak mod leak lg leak	0.0075 0.00125 0.0	0.0075 0.00125 0.0
"	"	"	greater than a shift	sm leak mod leak lg leak	0.009649 1.76E-5 0.0	0.00394 1.68E-5 0.0
"	"	status not commun	"	sm leak mod leak lg leak	0.009495 0.05 5.0E-4	0.004311 0.05 5.0E-4
"	process non-crit	status commun	less than a shift	sm leak mod leak lg leak	.0019 .006 .004	.0002 4.0E-4 6.1E-5
moderate	process non-crit	status commun	greater than a shift	sm leak mod leak lg leak	2.67E-4 0.0 0.0	2.67E-4 0.0 0.0
"	"	status not commun	"	sm leak mod leak lg leak	5.3E-4 0.0 0.0	5.0E-4 0.0 0.0
"	non-process critical	status commun	less than a shift	sm leak mod leak lg leak	0.005 5.0E-4 0.0	5.0E-4 5.0E-5 0.0
"	"	"	greater than a shift	sm leak mod leak lg leak	0.009217 7.8E-4 0.0	0.0013 1.3E-4 0.0
"	"	stuatus not commun	"	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
"	non-process non-crit.	commun stauts	less than a shift	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
"	"	"	greater than a shift	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
"	"	status not commun	"	sm leak mod leak lg leak	0.0 0.0 0.0	0.0 0.0 0.0
none	no leaks	no leaks	no leaks	no leaks	0.0	0.0

Process Leak Detection and Control (PLDC) System

PLDC can be performed both manually (operators) and automatically (system). The ability to detect and control process leaks are dependent upon the experience, knowledge and training of the operating crew, sensitivity of the detection, and reliability of the control system.

Errors are exacerbated by poorly engineered systems that invite errors. Such systems are difficult to construct, operate, and maintain (Ingles, 1985; Melchers, 1987; Moan, 1983). New technologies compound the problems of latent system flaws. Complex design, close coupling (failure of one component leads to failure of other components) and severe performance demands on systems increase the difficulty in controlling the impact of human errors even in well operated systems (Perrow, 1984). Emergency displays frequently have been found to give improper signals of the state of the systems (Lord Cullen Report, 1990; Perrow, 1984).

Human performance is a function of the lead time available to respond to warnings in the system. Errors are compounded by the lack of effective early warning systems. If the lead time is short, corrective action must be brief before the situation reaches a critical state. On the other hand, if the system is too sensitive causing frequent false alarms, operators will eventually cease to respond to the warning signals.

Management should invest in operator training (normal operating and crisis management), experience and knowledge, detection, (human-system interfacing, system communication and information) and emergency shutdown systems. These changes would result in better understanding of the process system and crisis management by front line operators. Cost-benefit analysis of the alternatives assist management in making choices which reduce risk and are cost effective.

An improved PLDC system was investigated involving improvements in the physical leak detection system, in the emergency shut-down system, fire suppression (deluge) systems. Similar PLDC improvement measures have been implemented in other industries (e.g. nuclear power and refineries) (Bell and Swain, 1981; Swain and Guttmann, 1983; Swain, 1988).

The influence of the improved PLDC program influence the frequency of explosions or fires and are summarized in Table 4. The results indicate improved detection and control systems could be expected to lead to a decrease in the number of explosions and fires by a factor of 2.5. Negligible reduction of fire and explosion event frequencies are observed for non-detected leaks.

Table 4
Probabilities of explosion or fire with and without an improved PLDC system

leak control	process leak detection	explosion or fire	P[expl or fire] (prior)	P[expl or fire] (post)
leak control	detected	fire	0.0075	0.002
"	"	explosion	0.0075	0.002
no leak control	"	fire	0.208	0.182
"	"	explosion	0.207	0.181
"	not detected	fire	0.435	0.435
"	"	explosion	0.435	0.435

CONCLUSIONS

Post-mortem studies provide a basis from which to construct probabilistic models (influence diagrams) of general classes of marine casualties. Analyses of post-mortem accident studies lead to a greater understanding of the effects of HOE in accident sequences. Though quantitative data may be limited in availability and detail they are not a replacement for using sound experience and judgment. Operators, engineers, managers, and regulators are able to make effective decision support evaluations of alternatives for managing HOE in operations of offshore production systems.

The results of the research project upon which this paper is based has indicated the following developments are needed to allow this approach to be integrated into engineering practice:

1) Further development and testing of a classification system for HOE.

2) Further development of a human and organizational factor database management system to interface with the HOE analytical models.

Work on these topics is continuing.

ACKNOWLEDGMENTS

This paper is funded in part by a grant form the National Sea Grant College Program, National Oceanic and Atmospheric Administration, Department of Commerce, under grant number NA89AA-D-SG138, project number R/OE-17 through the California Sea Grant College, and in part by the California State Resources Agency. The views expressed herein are those of the authors and do not necessarily reflect the views of NOAA or any of its sub-agencies. The U.S. Government is authorized to reproduce and distribute for government purposes.

This work also has been sponsored in part by Chevron Research & Technology Company and Chevron Shipping Company, Amoco Production Company and Amoco Transport Company, Unocal Corporation, the California State Lands Commission, the U.S. Coast Guard, the U.S. Minerals Management Service, and the American Bureau of Shipping. The support and guidance of these sponsors is gratefully acknowledged.

REFERENCES

Bea, R.G., and Moore, W.H., 1991, "Management of Human and Organizational Error in Operational Reliability of Marine Structures," *Proceedings, Society of Naval Architects and Marine Engineers 2nd Offshore Symposium: Designs and Codes.* Houston, TX. April.

Bell, B. J., and Swain, A. D., 1981, "A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants, Div. of Facility Operations", Office of Nuclear Regulatory Research, U. S. Nuclear Regulatory Commission, Report NUREG/CR-2254, Washington, D.C.

Howard, R.A, 1990, "From Influence to Relevance to Knowledge," From *Influence Diagrams, Belief Nets and Decision Analysis*, Ed. Oliver, M.R. & Smith, J.Q., Wiley & Sons: New York.

Ingles, O.G., 1985, "Human Error, and Its Role in the Philosophy of Engineering," Ph.D. Thesis, University of New South Wales, Australia.

Lee, B.S. & McMillan, W.S., 1992, "A Knowledge Based System for Offshore Permit to Work Management," *Proceedings, Second International Offshore and Polar Engineering Conference.* San Francisco.

Melchers, R.E., 1987, *Structural Reliability Analysis and Prediction*, Brisbane, Australia: Ellis Horwood Limited, Halsted Press, John Wiley & Sons.

Moan, T., 1983, "Safety of Offshore Structures," *Proceedings, of Fourth International Conference on Applications of Statistics and Probability in Soil and Structural Engineering.*

Moore, W.H., and Bea, R.G., 1992, "A Practical Human Error Taxonomy for Marine Related Casualties," Research Report No. 92-3, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering*, University of California, Berkeley. June.

Paté-Cornell, M. E., 1986, "Warning Systems in Risk Management," *Risk Analysis*, Vol. 6, No.2.

Paté-Cornell, M.E., 1992, "A Post-Mortem Analysis of the *Piper Alpha* Accident: Technical and Organizational Factors," Research Report No. 92-2, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering*, University of California, Berkeley. September.

Paté-Cornell, M.E., and Bea, R.G., 1989, "Organizational Aspects of Reliability Management: Design, Construction, and Operations of Offshore Platforms," Research Report no.89-1, Department of Industrial Engineering and Engineering Management, Stanford University.

Paté-Cornell, M. E., and Seawell, J.P., 1988, "Engineering Reliability: The Organizational Link," *Proceedings, ASCE Specialty Conference on Probabilistic Mechanics, Structural, and Geotechnical Safety.* Blacksburg, Virginia.

Perrow, C., 1984, *Normal Accidents: Living with High Risk Technologies*, New York: Basic Books, Inc.

Phillips, L.D., Humphreys, D.E., and Selby, D.L., 1990, "A Socio-Technical Approach to Assessing Human Reliability," From *Influence Diagrams, Belief Nets and Decision Analysis*, Ed. Oliver, M.R. & Smith, J.Q., Wiley & Sons: New York.

Roberts K.H. and Moore W.H., 1992, "The Gordian Knot: Into which sailed the *Exxon Valdez*," Research Report No. 92-1, Management of Human Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering, University of California, Berkeley.* January.

Swain, A. D. 1988, "Safety Analysis and Risk Assessment for Chemical Process Industry Practitioners: Human Reliability Analysis," American Institute of Chemical Engineers, New Jersey, Oct.

Swain, A. D., and Guttmann, H. E., 1983, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," Office of Nuclear Regulatory Research, U. S. Nuclear Regulatory Commission, Report NUREG/CR-1278, Washington, D. C.

United Kingdom Department of Energy, 1990, *The Public Inquiry into the Piper Alpha Disaster, The Hon Lord Cullen*, Vol. 1 & 2, HMSO Publications, London. November.

United Kingdom Department of Energy, 1988, *Piper Alpha Technical Investigation: Further Report.* Petrie Report. Crown: London. December.

Ship Structures Symposium '93

November 16-17, 1993
Sheraton National Hotel, Arlington, Virginia

IMPROVING THE MANAGEMENT OF HUMAN AND ORGANIZATION ERRORS (HOE) IN TANKER OPERATIONS

William H. Moore[1] , Robert G. Bea[2] , Karlene H. Roberts[3]

ABSTRACT

Human and organization errors (HOE) account for the vast majority of unanticipated significant problems associated with the design, construction, and operation of ships. Approximately 80 % of the problems are due to HOE, and approximately 80% of these can be traced to operations. The authors have developed a qualitative and quantitative approach to the evaluation of HOE in the operations of crude carriers. This paper summarizes the results of this work in the context of an analysis of the Exxon Valdez *incident. The HOE improved management approach is illustrated with evaluation of several alternatives to minimize the frequency of such incidents.*

INTRODUCTION

The study on which this paper is based is a three-year study to develop a "first generation" engineering procedure to help address and evaluate alternative improvements in the management of human and organization errors in the operations of marine systems. This study has accessed and evaluated existing databases that address major marine accidents including some 700 individual accident reports. Existing systems to classify and describe HOE have been evaluated and a system specially adapted to marine operations has been proposed. A complimentary qualitative - quantitative HOE analysis procedure has been developed. The procedure has been applied to two recent high consequence accidents: the grounding of the *Exxon Valdez* and the Occidental *Piper Alpha* platform explosions and fires. Two forward looking HOE studies have been conducted; one addresses tanker discharge operations and the other addresses platform crane operations.

---

[1] Marine Systems Engineer, Dept. of Naval Architecture & Offshore Eng., 207 Naval Architecture Bldg., University of California at Berkeley, CA 94720

[2] Professor, Dept. of Naval Architecture & Offshore Engineering and Dept. of Civil Eng., 212 McLaughlin Hall, University of California at Berkeley, CA 94720

[3] Professor, Haas School of Business, 350 Barrows Hall, University of California at Berkeley, CA, 94720

The following summarizes the primary observations that were developed during this study:

- There are three primary players in high consequence accidents: the front-line operators of the system (humans), the groups that are responsible for the management of the systems (organizations), and the physical elements (system).
- High consequence accidents result from a multiplicity or compounding sequence of break-downs in the human, organization, and system; often there are "precursors" or early warning indications of the break-downs that are not recognized or ignored.
- Systems (physical components) are generally the easiest of the three components to address; design for human tolerances and capabilities (ergonomics), provision of redundancy and damage / defect tolerance, and effective early warning systems that provide adequate time and alerts so that systems can be brought under control are examples of potential measures. Error inducing systems are characterized by complexity, close coupling, latent flaws, small tolerances, severe demands, and false alarms.
- Humans are more complex in that error states can be developed by a very wide series of individual characteristics and "states" including fatigue, negligence, ignorance, greed, folly, wishful thinking, mischief, laziness, excessive use of drugs, bad judgment, carelessness, physical limitations, boredom, and inadequate training. External (to the system) and internal (in the system) environmental factors such as adverse weather, darkness, smoke, and heat provide additional influences. Selection (determination of abilities to handle the job), training (particularly crisis management), licensing, discipline, verification and checking, and job design provide avenues to improve the performance of front-line operators.
- While the human and system aspects are very important, the organization aspects frequently have over-riding influences; corporate "cultures" focused on production at the expense of quality, ineffective and stifled communications, ineffective commitment and resources provided to achieve quality, excessive time and profit pressures, conflicting corporate objectives, and counter-quality and integrity incentives are often present in "low reliability" organizations. Generally, these aspects are the most difficult to address. Experience indicates that high reliability organizations tend to improve, while low reliability organizations do not improve rapidly, if at all.
- The most important part of the HOE evaluation process is *qualitative*; a realistic and detailed understanding of the human, organization, and system aspects and potential interactions must underlie the entire process. Quantitative aspects provide an important framework in which to evaluate the potential effectiveness of proposed "fixes" and to examine the detailed interactions of human, organization, and system components.
- There is no marine system HOE database that can be relied upon to give accurate quantitative indications of the frequencies of accident contributors; in the case of specific accident scenarios, existing databases frequently give misleading indications of causes and consequences. Complex interactions are frequently not determined or lost in the reporting. Study of past high consequence accidents can provide important insights into the complex interactions of humans, organizations, and systems and can provide the basis for development of generic "templates" for evaluation of other similar systems. Study of "near misses" can show how potentially catastrophic sequences of actions and events can be interrupted and brought under control. There is no generally available database or archiving system for "near miss" information.
- An adequate and understandable quantitative analysis system exists to assist evaluations of HOE; probability based "influence diagramming" has proven to be able to show the complex interactions and influences and efficiently produce quantitative indices that can indicate the effectiveness of alternative HOE "fixes." Because of the lack of accurate and

definitive objective data to serve as input to such quantitative models, structured "index" models have been developed to allow encoding subjective judgment into the evaluation of probabilities.

- A reasonable and workable HOE classification system has been developed. This system should provide the basis for development of future marine operations accident reporting systems. Investigators need to be well trained in the evaluation of human and organization factors in marine accidents. An industry wide computer database system needs to be developed to improve the efficiency of accident reporting and analysis of results. Information on both accidents and "near misses" need to be incorporated into this database.

- The primary objective of HOE analyses should not be to produce numbers. The primary objective of HOE analyses should be to provide a disciplined and structured framework that is able to produce insights and information that can lead to improvements in the management of HOE.

A GORDIAN KNOT

The principal focus of post-accident (or post catastrophe) investigations has been on performance failures that immediately preceded an accident. These are termed *active failures:* human errors or violations having an immediate impact on the integrity of a system. More recently, however, the scope of accident inquiries has widened considerably to also include *latent failures* committed in design, management, and organization [Reason, 1990]. This broader scope of accident investigation is recognized in the model presented here (Figure 1), particularly in Figure 2 which lays out the active failures, and Figure 3 which addresses latent failures.

Latent failures in technical systems--human errors or violations committed within the design, management, and organization of large scale systems--have recently been identified, and compared to resident *pathogens* in the human body which combine with local triggering factors (i.e., life stresses, toxic chemicals, etc.) to overcome the immune system (i.e., system safety measures) and produce disease (i.e., errors):

> *Like cancers and cardiovascular disorders, accidents in defended systems do not arise from single causes. They occur because of the adverse conjunction of several factors, each one necessary but none sufficient to breach the defenses...As in the case of the human body, all technical systems will have some pathogens lying dormant within them* [Reason, 1990; pg. 74].

The likelihood of an accident, or of a system's propensity for error, can therefore be described as a function of the number of pathogens in the system. The more abundant the pathogens, the greater the probability that some of them will encounter just that combination of local triggers necessary to complete a latent accident sequence. Further, the more complex the system, the more pathogens it will contain. The key assumption, however, is that *resident pathogens can be identified proactively, given adequate access and system knowledge* [Reason, 1990]. A qualitative analysis of the events leading to the grounding of the *Exxon Valdez* identified a number active failures, some of which are identified in Figure 2, and pathogens, some of which are identified in Figure 3.

When *Exxon Valdez* hit Bligh Reef just after midnight on March 24, 1989 she was holed in eight of her eleven cargo compartments and two ballast tanks. Most of the cargo loss occurred during the first eight hours after grounding. Thirty minutes after the grounding 115,000 of the 1,263,000 barrels were lost. A total of 258,000 barrels, or eleven million

gallons, were lost in all. Many of the elements represented in the formal model are suggested by the story of what happened.

Our discussion will focus only on possible latent factors to leaving the Traffic Separation Scheme (TSS) and failing to return. A complete analysis would recognize the involvement of many parties over a long period of time, and a number of other behaviors. Table 1 summarizes the primary contributors to the deviation from the TSS by the *Exxon Valdez* crew and are described in this section.

Deviation from the TSS

A number of external factors potentially contributed to this act. While the weather was good, one physical factor was the possibility that an ice floe had moved into the outbound TSS. Other factors possibly came into play.

Deviation might have reduced travel time, an economic factor. Deviation was not uncommon, suggesting that a culture of reliability was possibly not in place. But it also suggests that the checks and balances often used in systems to insure that required behaviors are obtained did not exist. External sources might have warned against deviation. As we discuss later, the Coast Guard Vessel Traffic Service had atrophied over time in that equipment maintenance and VTS staffing were both limited. Both of these limitations might have been overcome if a pilot had stayed with the ship until she came closer to clearing the Sound.

In addition, behavior at sea the night of the grounding indicated that various parties to the situation failed to act on some fairly clear warning signals. Ironically, three months before this accident, the only other major spill in the twelve years of the Trans-Alaska Pipeline operation occurred when the *Thompson Pass* released 1,700 barrels of oil. Other accidents had happened other places, yet all parties to tanker operation in Valdez Harbor seemed oblivious to these warning signals.

Failure to return to the TSS

The immediate active errors contributing to this failure were the actions of the third mate and the helmsman on the bridge. Both failed to recognize the ship's location.

A number of latent failures underlie these active failures. Again, due to time constraints only a few are mentioned here. Exxon Shipping Company recognized that the helmsman had limited capability. The company had been unsuccessful with the union in limiting his duties so he could not take the helm of the ship. Both the company and the union had some responsibility to examine their bargaining and negotiation within the framework of improving safety in tanker operation.

While either a training or selection problem (or both) may be additional pathogens, the context within which these people operated strongly suggests yet others. The captain was off the bridge and before departing had asked the third mate if he felt he could take the ship out of the Sound. It is possible the pressure the captain felt to complete paper work helped him come to a poor decision to be off the bridge. But certainly, the captain's experience and training should have suggested too him that the "proper" answer to asking a subordinate, "can you do the job?" is "yes." Again, apparently expediency overrode the operation of a safe and reliable culture in determining behavior.

We turn from this limited illustration of the complex qualitative analysis underlying model development to the model itself.

MODELING THE TANKER GROUNDING

Based on the results summarized in the foregoing section, the accident events are categorized in to underlying/contributing, direct, and compounding factors. The primary contributing factors are shown in Figure 1 and summarized as follows.

Underlying / Contributing Factors

Event: *Exxon Valdez* deviates from the outbound *traffic separation scheme* (TSS) to avoid an ice floe in the outbound lane.

Causes: The deviation of from the TSS was not an isolated incident though was not recommended by either the operators nor the USCG. At the time of the grounding there had been a reduction of billets at the USCG Marine Safety Office in Valdez. On the night of the grounding the vessel traffic center (VTC) crew had not established *Exxon Valdez* on the radar nor kept in radio communication after the vessel departed from the Valdez Narrows.

As the vessel deviated from the lane it was placed on automatic pilot (it is questionable as to whether the auto pilot was on until just before the grounding).

The master left the bridge leaving only the third mate in command which is in violation of Exxon Shipping operating policy. At the time of the grounding, Exxon was in the process of determining how to reduce the crew sizes aboard the vessels even though crews frequently are excessively fatigued and overworked. The chief mate was too tired to take his watch at 12 midnight since he had spent the day coordinating the loading of the vessel at the Alyeska terminal. The company had conducted no studies on the human effects of reducing crew sizes.

Conditions: Ice floe conditions in the outbound lane of the TSS was a precursor to the decision to deviate from the TSS.

Direct Factors

Event: The vessel does not return to the TSS and grounds on Bligh Reef.

Causes: The USCG had problems with the radar system in Prince William Sound at the time of the grounding. It is questionable as to whether the VTS personnel could properly monitor the *Exxon Valdez* on the radar. Though no radar communication may have been possible, vessel and VTS personnel had not kept in radio communication to determine the track of *Exxon Valdez*.

The third mate was unable to determine the location of the vessel just before the grounding. His lack of knowledge, training, and experience under these operating conditions had made it difficult to make proper navigation decisions.

Conditions: The time of day was approximately midnight at or about the time of a change of watch on the bridge.

Compounding Factors

Event: Captain Joseph Hazelwood, the master of *Exxon Valdez*, attempts to lodge or dislodge the vessel from Bligh Reef resulting in the compounded loss of cargo.

Cause: Captain Hazelwood may have attempted to push the vessel onto the reef to keep the vessel from capsizing. This may have been in violation of laws limiting the discharge of cargo into the water.

Conditions: At the time of the grounding the tide was dropping. This may have led to the decision to stabilize the vessel on the rocks to prevent capsizing.

Model Representation

This model incorporates critical factors both aboard *Exxon Valdez* and at the Vessel Traffic Center (VTC) in Valdez. The underlying/contributing event is the deviation of the vessel from the Traffic Separation Scheme (TSS). The grounding of the vessel is the direct/initiating event and the attempt to dislodge the vessel from the rocks is the subsequent compounding event that led to the additional loss of cargo. Figure 2 diagrams the influences between error solicitors (events, decisions, and actions) leading to the grounding.

Intermediate events, decisions and actions are related to the primary events and directly influence the grounding events. Conscious actions and decisions were made by the master to: (1) deviate from the TSS, (2) depart from the bridge during transit, and (3) place the tanker on auto pilot and "load up" program. Each of these actions and decisions are represented as decision nodes.

The direct influences of HOE and environmental causes on primary and intermediate events, decisions and actions are shown in the final representation in Figure 3. The grounding model forms a basis from which the influence diagram template is developed.

Influence Diagram of Vessel Grounding or Collision

Once a vessel deviates from a specific TSS within navigable waters, potential hazards (vessel traffic, reefs, currents, etc.) can greatly increase the risk of transit. An underlying factor in the events leading to the grounding of *Exxon Valdez* was the decision to deviate from the TSS. Thus the accident has been classified under groundings and collisions. In analyses of tanker groundings and collisions, the following general questions are addressed in developing the influence diagram template models.

- Did the vessel deviate from a previously established traffic scheme? If so, was it a conscious decision to do so? It is assumed in the model that conscious decisions were made to deviate from the scheme and was not inadvertent.
- Is the path and location of the vessel being properly monitored? Monitoring can be either internal (vessel crew) or internal and external (vessel traffic center). The monitoring of the vessel is directly related to whether a grounding or collision will occur.
- Were environmental factors involved in the decision to deviate from the traffic separation scheme (ice in the lane, waves, tide, etc.)? Was vessel traffic a factor in the decision to deviate from the traffic scheme?
- Are ship system factors involved in the grounding of the vessel? For example, the vessel may loose power, steering, or navigation capabilities? (This issue has been of particular concern in such tanker groundings as the *Amoco Cadiz* off the coast of France and the *Braer* off of the Shetland Islands.)
- Were human and organizational errors involved in the decision to deviate from the traffic separation scheme and/or monitoring of vessel path?

MODELING THE TANKER GROUNDING

Based on the results summarized in the foregoing section, the accident events are categorized in to underlying/contributing, direct, and compounding factors. The primary contributing factors are shown in Figure 1 and summarized as follows.

Underlying / Contributing Factors

Event: *Exxon Valdez* deviates from the outbound *traffic separation scheme* (TSS) to avoid an ice floe in the outbound lane.

Causes: The deviation of from the TSS was not an isolated incident though was not recommended by either the operators nor the USCG. At the time of the grounding there had been a reduction of billets at the USCG Marine Safety Office in Valdez. On the night of the grounding the vessel traffic center (VTC) crew had not established *Exxon Valdez* on the radar nor kept in radio communication after the vessel departed from the Valdez Narrows.

As the vessel deviated from the lane it was placed on automatic pilot (it is questionable as to whether the auto pilot was on until just before the grounding).

The master left the bridge leaving only the third mate in command which is in violation of Exxon Shipping operating policy. At the time of the grounding, Exxon was in the process of determining how to reduce the crew sizes aboard the vessels even though crews frequently are excessively fatigued and overworked. The chief mate was too tired to take his watch at 12 midnight since he had spent the day coordinating the loading of the vessel at the Alyeska terminal. The company had conducted no studies on the human effects of reducing crew sizes.

Conditions: Ice floe conditions in the outbound lane of the TSS was a precursor to the decision to deviate from the TSS.

Direct Factors

Event: The vessel does not return to the TSS and grounds on Bligh Reef.

Causes: The USCG had problems with the radar system in Prince William Sound at the time of the grounding. It is questionable as to whether the VTS personnel could properly monitor the *Exxon Valdez* on the radar. Though no radar communication may have been possible, vessel and VTS personnel had not kept in radio communication to determine the track of *Exxon Valdez*.

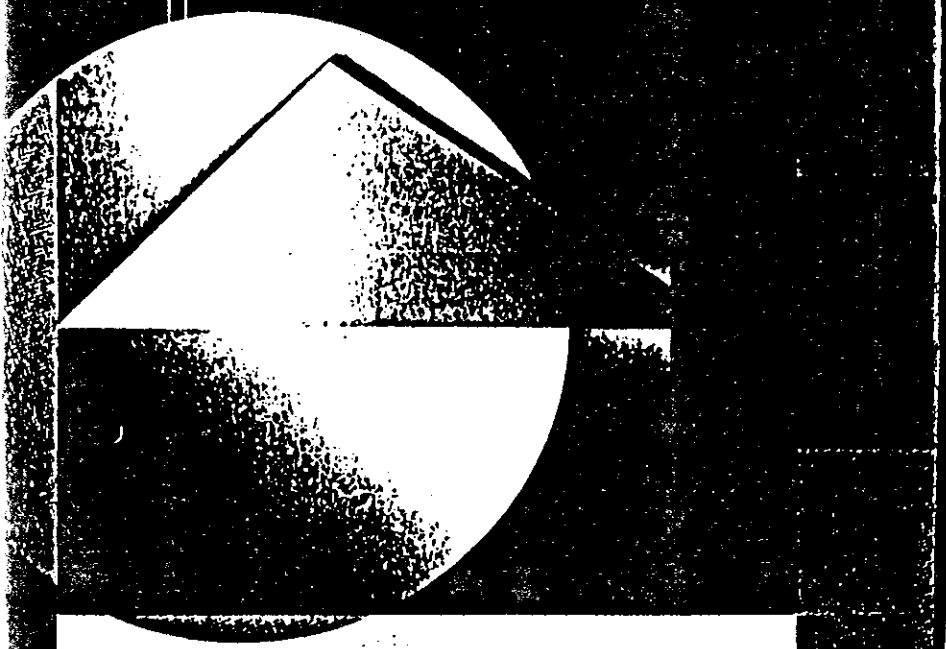
The third mate was unable to determine the location of the vessel just before the grounding. His lack of knowledge, training, and experience under these operating conditions had made it difficult to make proper navigation decisions.

Conditions: The time of day was approximately midnight at or about the time of a change of watch on the bridge.

Compounding Factors

Event: Captain Joseph Hazelwood, the master of *Exxon Valdez*, attempts to lodge or dislodge the vessel from Bligh Reef resulting in the compounded loss of cargo.

NEW CHALLENGES TO UNDERSTANDING ORGANIZATIONS



KARLENE H. ROBERTS

NEW CHALLENGES TO UNDERSTANDING ORGANIZATIONS

Karlene H. Roberts examines the management of "high reliability" organizations that dramatically affect economies, corporations, and human life. Roberts, consultant to the Joint Chiefs of Staff, has assembled some of the world's most recognized researchers to create what is destined to become a landmark publication.

Learn how mistakes contributed to the Tenerife air crash and the grounding of the *Exxon Valdez*, and how new paradigms and models can help prevent these disasters.

ISBN 0-02-402052-4

9 780024 020529 90000>

The influence diagram shown in Figure 4 is representative of the primary contributing factors for a vessel grounding or collision. The grounding of *Exxon Valdez* falls within this general class of accidents. The primary contributors are described below and the variables are summarized in Table 2.

- *Environmental conditions.* The environmental operating conditions are described as a state variable since the conditions will vary from time of day to season.
- *Human errors.* Human errors are affected by the environmental operating conditions, the deviation from the traffic lane (non-routine) and vessel traffic (stress and non-routine). These are described as a probabilistic variable.
- *Deviates traffic separation scheme.* The vessel may deviate the traffic separation scheme as a result of environmental factors or vessel traffic. The deviation is represented as a probabilistic variable.
- *Vessel traffic.* Vessel traffic will be variable dependent upon the location and inherent variability in shipping throughput. Vessel traffic is represented as a probabilistic variable to accommodate these contributing factors.
- *Monitor vessel path:* Monitoring of vessel path and location is affected by deviation from the TSS and human errors. Vessel paths are closely monitored if deviation occurs.
- *Vessel operation system failure.* Vessel operating system failure is included to account for possible loss of systems critical to the safe operation of the vessel. This includes navigational devices, power plant, or any other critical operating system. The failure of these systems are variable and are represented as a probabilistic node.
- *Grounding or collisions.* Groundings or collisions are directly affected by vessel traffic, TSS deviation and monitoring of vessel path, and operational system failure. The failure event is considered probabilistic upon the contributing factors.
- *Spill.* The possibility of a spill is contingent upon the grounding or collision of the vessel and its speed at the time of the casualty event.
- *Vessel speed.* The vessel speed will have a direct effect upon the outflow of oil upon grounding or collision.
- *Spill cost.* The cost of the spill is represented as an expected value node to be evaluated at the end of the diagram.

Evaluating the Grounding and Collision Model

In evaluating the influence diagram shown in Figure 4, the two particular values of concern are the probabilities of groundings or collisions given human errors and the expected costs of a spill. Human error probabilities were derived using the *Human Error Safety Index Method* (HESIM) developed by Moore and Bea (1993). The HESIM integrates error inducing parameters (error solicitors) leading to a potential accident event. The error solicitors are organizational, human, task, system, and environmental factors. The HESIM is further described in Appendix B. The USCG casualty database and human error modeling for nuclear power plants were also used to determine contributing factors influencing tanker casualties (e.g., machinery and equipment failures, human error task errors, etc.) [CASMAIN, 1990; Swain & Gutumann, 1983]. Spill size data were determined from VLCC collision and grounding models [Det Norske Veritas, 1991]. The probabilities of spill sizes for a grounding or collision of a standard VLCC are provided in Table 3.

Environmental operating conditions will differ from season to season and vessel traffic is dependent upon location of the study. Sensitivity analysis may be performed on these vari-

ables to determine the impact of the variations in the conditions. For the model the nominal values for environmental operating conditions and vessel traffic in the Valdez port are summarized in Table 4.

Human errors are dependent upon three primary contributing factors: (1) vessel traffic, (2) vessel deviation from the TSS, (3) and the environmental operating conditions. The three contributing factors. The human errors at the operator level are described for a well operated tanker fleet with a high commitment to safety and resources made available for safe operation. Heuristic judgments were used to determine the frequencies of HOE's under the various operating conditions.

Vessel groundings and collisions are directly dependent upon vessel path monitoring, deviation from the TSS, vessel system failure. It is assumed if the vessel path is properly monitored, human intervention will prevent a collision or grounding course. A vessel operating system failure is presumed to be only 1 out of 100 transits (.01). Vessel operating speeds in the areas of vessel traffic are presumed to be 5 knots 70% of the time and 30% of the transits are at 10 knots.

Spill costs are estimated at $30,000 per barrel (bbl).[1] These estimates are based on costs of clean up, legal, and miscellaneous costs. Evaluating the influence diagram results in a the annual probability of groundings and collisions and probabilities of human errors given the grounding or collision are shown in Table 5.[2] There is a 1.1% chance of either a collision or grounding per year. The largest contributors to the grounding and collision events are lack of communication or information, violations, and mental-physical lapses. These three contributors account for over 50% of the human error related causes.

The Oil Pollution Act of 1990

Since the grounding of *Exxon Valdez*, the most influential changes for tanker operations in U.S. territorial waters has been the *Oil Pollution Act of 1990* (OPA 90). OPA 90 addresses a wide variety of tanker operation issues and are representative of current HOE management alternatives [Noble, 1993]. As an overview, Title IV of OPA 90 [Connaughton, 1990]:

- mandates that the Coast Guard tie into the National Driving Register to detect individuals with drunk driving convictions;
- increases Coast Guard authority to deny or revoke mariner licenses and documents;
- authorizes removal of incompetent personnel;
- increases Coast Guard authority to deny entry of foreign vessels into the U.S. waters on the grounds of deficient manning;
- limit crew work hours aboard tankers to 15 hours per day but no more than 36 hours in any 72 hour period;
- mandates the Coast Guard conduct studies on vessel traffic and tanker navigation;

---

[1] The cost of the *Exxon Valdez* was approximately $30,000 per barrel spilled. Many contributing factors affect the cost per barrel; such as spill location, size, type of oil (product or crude), clean-up procedure, legal fees, etc. Cost estimates can be modified to incorporate as many contributors as wanted. The spill costs could have been modeled as a probabilistic node to incorporate the uncertainty involved in determining the total costs. However, for simplicity we have set a deterministic value of $30,000 per barrel spilled.

[2] The human error probabilities are the probabilites that the error was the primary contributor. Other human errors may be observed in the accident sequence.

- requires all new tanker builds to be double-hulled in addition to the phasing out of existing tankers beginning in 1995 and concluding in 2010; and,
- require the Coast Guard to designate areas where two licensed personnel are required on the vessel bridge and tug escorts are necessary.

There are three fundamental complimentary forms of HOE management alternatives to improve operational reliability: 1) directly addressing HOE through HOE management programs, 2) changes in operational procedures, and 3) development of human error tolerant systems. The HOE management alternative described here is a change of operational procedure. The HOE management alternative modeled is the required tug vessel support specified by the *Oil Pollution Act of 1990* (OPA 90).

Figure 5 is an influence diagram representing the addition tug support to tank vessels for transit through navigable waters. The tug support is presumed available during all environmental conditions except for high seas (waves). In the event of a vessel system failure the tug support is available. It is presumed that the tug(s) escort the vessel and are monitor the vessel path.

The effect of the tug support is an increase in the probability of reliable monitoring of vessel path and a reduction of the probability of grounding or collision. The estimated reductions in human error frequencies were developed through expert judgments and reference to studies performed for nuclear power plant operations [Swain & Guttmann. 1983]. It is assumed the primary reductions in human errors at the operator level are in violations, communication and information, mental-physical lapses, and knowledge, training, and experience. Tanker crews are less willing to violate transit laws when tugs are present (regulating and policing). Communication and information are more available to the tanker crews, since the tug crews are knowledgeable of the waters being transited. The experiences of the tug crews also reduces problems of knowledge training and experience of the tanker crews. Mental and physical lapses are less likely to occur if proper communication and information as to the status of the tanker vessel is being exchanged between tanker and tug crews.

Evaluating the influence diagram in Figure 5 to find the probability of groundings and collisions and probabilities of human errors given the grounding or collision are shown in Table 6. The probability of collisions have been reduced by 57% and the probability of groundings are reduced by 75% if tug support is available. There is a net expected benefit of $11,309,096 if tug support is available.

Substantial reductions in the incidence of human errors as the primary accident related cause are observed. The incidence of violations as primary cause have been reduced by 75% for collisions and 56% for groundings. Communication and information errors and mental-physical lapses have been reduced by more than 82% for collisions and 67% for groundings. Initiations of accidents resulting from human system interface errors for collisions and groundings are reduced by 85% and 75% respectively.

The addition of tug escorts for vessels for specified transits reduce the incidence of grounding or collision events. Other alternatives may be addressed to determine the impact upon the system.

CONCLUSIONS

We have developed an engineering procedure to systematically address HOE in operations of tankers. The case study of the grounding of the *Exxon Valdez* has been used as a

framework from which to develop qualitative and quantitative models (influence diagram templates) to address groundings and collisions which are similar in nature. The template models are used to assist engineers, operators, regulators, and managers in evaluating alternatives to reduce the impacts of human and organizational errors in the operations of marine systems.

The template models involve both qualitative and quantitative assessments. Due to the deficiencies in existing HOE databases, the quantitative models rely heavily on experience and judgments. Our experience with applications of this procedure to operations of marine systems indicates that if qualified and motivated personnel are involved in the analyses, the procedure can produce important insights on how best to utilize safety resources to help reduce the incidence and effects of HOE in operations of marine systems

ACKNOWLEDGMENTS

This paper is funded in part by a grant from the National Sea Grant College Program, National Oceanic and Atmospheric Administration, Department of Commerce, under grant number NA89AA-D-SG138, project number R/OE-17 through the California Sea Grant College, and in part by the California State Resources Agency. The views expressed herein are those of the authors and do not necessarily reflect the views of NOAA or any of its sub-agencies. The U. S. Government is authorized to reproduce and distribute for government purposes.

This work also has been sponsored in part by Chevron Research & Technology Company and Chevron Shipping Company, Amoco Production Company and Amoco Transport Company, Unocal Corporation, the California State Lands Commission, the U. S. Coast Guard, the U. S. Minerals Management Service, and the American Bureau of Shipping. The support and guidance of these sponsors is gratefully acknowledged.

REFERENCES

Bodily, S.E. 1985. *Modern decision making: A guide to modeling with decision support systems.* McGraw Hill Inc.

CASMAIN. 1991. USCG casualty database. 1981-1990.

Connaughton, S.T. 1990. Vessel pollution prevention and response considerations. *New Oil Pollution Act of 1990 Conference.* Government Institutes, Inc.

Det Norske Veritas. 1991. Comparative study on potential oil spill in collision and/or grounding - different tanker designs. *Tanker Spills: Prevention by Design.* Appendix F. Committee on Tank Vessel Design, Marine Board Commission on Engineering and Technical Systems. National Academy Press: Washington, D.C.

Howard, R.A. 1990. From influence to relevance to knowledge. From *Influence Diagrams, Belief Nets and Decision Analysis.* Edited by Oliver, M.R. & Smith, J.Q. Wiley & Sons: New York. pp. 3-24.

Howard, R.A. & Matheson, J.E. 1981. Influence diagrams. In *The principles and applications of decision analysis.* Vol. II (1984). R.A. Howard and J.E. Matheson (eds.). Strategic Decisions Group, Menlo Park, CA.

Moore, W.H. & Bea, R.G. 1993. Management of human error in operations of marine systems: Final project report. Research Report No. HOE-93-1, Management of Human

Error In Operations of Marine Systems Project, *Department of Naval Architecture and Offshore Engineering*, University of California at Berkeley.

Noble, P. G. 1993. Safer Transport of Oil at Sea: A Social Responsibility for Naval Architects and Marine Engineers. *Marine Technology*, Vol. 30, No. 2, April.

Phillips, L.D., Humphreys, D.E. & Selby, D.L. 1990. A socio-technical approach to assessing human reliability. From *Influence Diagrams, Belief Nets and Decision Analysis*. Edited by Oliver, M.R. & Smith, J.Q. Wiley & Sons: New York. 1990. pp. 253-276.

Reason, J. 1990. *Human Error*. Cambridge University Press: New York.

Swain, A. D. & Guttmann, H. E. 1983. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications: Final Report, *NUREG/CR-1278*, U.S. Nuclear Regulatory Commission, Washington, D. C., August.

APPENDIX A: INFLUENCE DIAGRAMS[3]

One method of developing accident framework models for PRA analysis is through the use of *influence diagrams*. Influence diagramming is a form of PRA modeling which allows great flexibility in examining HOE and HOE management alternatives. There are distinct advantage for using influence diagrams as an alternative to standard event/fault tree analyses. In standard decision tree analysis, decisions are based on all preceding aleotory and decision variables [Howard & Matheson, 1981]. However, all information is necessarily available to a decision maker. In addition, information may come from indirect sources or may not come in the specific order in which the decision tree is modeled. It is not necessary for all nodes to be ordered in an influence diagram. This flexibility allows for decision makers who agree on common based states of information, but differ in ability to observe certain variables in the diagram modeling [Howard & Matheson, 1981]. Influence diagrams are able to organize conditional probability assessments required to determine unconditional probabilities of failures of specified target events [Phillips, *et al.*, 1990].

As described by Howard (1990) (see Figure A-1), the components of an influence diagram are: (1) *decision* and *chance nodes*, (2) *arrows*, (3) *deterministic nodes*, and (4) *value nodes*. Decisions are represented by square nodes which can be a continuous or discrete variable or a set of decision alternatives. Uncertain events or variables are represented by circular or oval chance nodes. Chance nodes can be continuous or discrete random variables or a set of events. Arrows indicate relationships between nodes in the diagram. Arrows entering a chance node signify that the probability assignments of the node are conditional upon the node from which the arrow originated. Deterministic nodes are those in which outcomes depend deterministically upon its predecessors. A value node is designated by the author to be: "the quantity whose certain equivalent is to be optimized by the decisions" of which only one node may be designated in the diagram. Value nodes may be a distribution of possible values. This is represented by a rounded edge single-border node. The value node may also be represented as the expected value. These nodes are represented by a rounded edge double-border rectangle.

---

[3] The *influence diagram* is defined by Bodily (1985) as:

> *"...a display of all of the decisions, intermediate variables, outcome attributes that pertain to a problem, along with the influence relationships among them. By influence we mean a dependency of a variable on the level of another variable."*

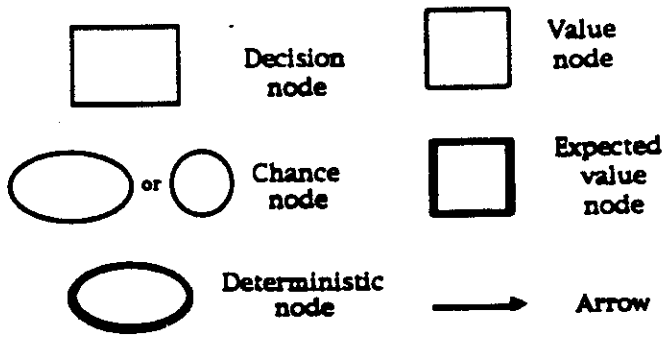


Figure A-1: Influence diagram characterizations

APPENDIX B: HUMAN ERROR SAFETY INDEX METHOD (HESIM)

Safety (risk) index methods are described as a modified quantitative risk assessment in which key risk contributors are identified, assessed and assigned numerically weighed values [Gale, 1993]. In absence of probabilistic data, determining safety indices allow for examination of the relative risks. As probabilistic information becomes available, comparisons are drawn between safety indices and probabilities of failure. This verification of risk indices leads to better probabilistic assessments if data is not available by implementing a safety index.

The HESIM accounts for contributing human, organizational, and system errors leading to human errors at the operational level [Moore & Bea, 1993]. The HESIM integrates error inducing parameters (error solicitors) leading to a potential accident event. The error solicitors are organizational, human, task, system, and environmental factors. The concept for the HESIM is to incorporate error factors from four general contributors: (1) organizational, (2) human, (3) system complexity, and (4) the operating environment. Organizational errors are further distinguished into top-level and middle-front-line management, and regulatory contributors. Human factors include the stress and "routineness" of the activity. Operating environment is differentiated into external operating environment (wind, waves, temperature, etc.) and internal operating environment (noise, fumes, smoke, etc.).

The *human error safety index* ($SI(HE_i|EDA_q)$) (Eqn. 1) for a particular event, decision, or action q (EDA_q) is the product of four safety indices: (1) the *organizational error index* ($SI_{HE_i|OE}$), (2) the *human factor index* ($SI_{Hum\ factor}$), (3) the *system index* (SI_{System}), and (4) the *environmental index* ($SI_{Environ}$).

$$SI[HE_i|EDA_q] = SI_{HE_i|OE,EDA_q} * SI_{HE_i|Hum\ factor,EDA_q} * SI_{HE_i|System,EDA_q} * SI_{HE_i|Environ,EDA_q} \quad \text{.....(B-1)}$$

Each safety index is assigned a value between 0 and 1 ($0 < SI < 1$) dependent upon the contribution of that factor upon the human error for particular events, decisions, or actions. The assigned values are acquired from accident data and heuristic judgments.[4]

[4] For further detail on the HESIM, see: Moore, W.H. & Bea, R.G. (1993) *Management of human error in operations of marine systems: Final project report.*

Table 1: Contributing factors to the grounding of *Exxon Valdez*

Deviation from TSS
• Possibility of ice floe • Reduction in travel time • Organizational culture of reliability was not in place • Checks and balances non-existent • VTS equipment maintenance and staff limited • Failure to pay attention to warning signals
Failure to return to TSS
• Third mate and helmsman fail to recognize location • Helmsman's limited capability: training and selection • Management and union negotiation activities fail to see safety as primary concern • Master's failure to monitor third mate

Table 2: Outcomes within each node of vessel grounding-collision influence diagram

vessel speed *5 kts* *10 kts* **vessel traffic** *light* *heavy*	**spill size (bbls)** *0-178,000* **grounding /collision** *none* *grounding* *collision*	**environment / operating conditions** *none* *lane obstruction* *waves* *wind* *tide*	**human errors** *none* *violations* *communication/information* *job design* *mental/physical lapse* *knowledge/experience/training* *human/system interfaces*
vessel operating system condition *operating* *fail*	**deviates vessel TSS** *no TSS deviation* *TSS deviation*	**monitor vessel path** *monitor* *no monitor*	

Table 3: Conservative discharge estimates for tanker groundings and collisions for fully loaded VLCC single-hull design[5]

Casualty event	Probability	Spill size in barrels (bbls)
Collision	.22	12,750
	.28	25,500
	.25	38,250
	.20	59,497
	.05	178,000
Grounding (5 kts)	.2	25,500
	.35	35,700
	.3	51,000
	.15	76,500
Grounding (10 kts)	.08	71,400
	.5	91,800
	.3	112,200
	.12	122,400

[5] Standard VLCC design with a 330,000 dwt capacity, 315 m long, 57.2 m breadth, 20.8 meter draft, .83 block coefficient.

Table 4: Nominal probabilities for tanker operating conditions

Environmental operating conditions:	Probability
none	.900
lane obstruction	.002
waves	.005
wind	.010
tide	.083
Vessel traffic	
light	.75
heavy	.25

Table 5: Annual probabilities of groundings and collisions and associated human errors for each event[6]

Event	P[Event]	
collision	.007	
grounding	.004	
Human Error	**P[human error| collision]**	**P[human error| grounding]**
none	.46	.42
violation	.08	.09
communication - information	.14	.15
job design	.08	.07
mental - physical lapse	.11	.12
knowledge - training - experience	.06	.07
human system interface	.07	.08

Table 6: Annual probabilities of grounding or collision event with tug support[7]

Event	P[Event]	
collision	.003 (-57%)	
grounding	.001 (-75%)	
Human Error	**P[human error| collision]**	**P[human error| grounding]**
none	.88 (91%)	.81 (93%)
violation	.02 (-75%)	.04 (-56%)
communication - information	.02 (-85%)	.03 (-80%)
job design	.03 (-63%)	.03 (-57%)
mental - physical lapse	.02 (-82%)	.04 (-67%)
knowledge - training - experience	.02 (-67%)	.03 (-57%)
human system interface	.01 (-85%)	.02 (-75%)

[6] These probabilities account for the primary causes of the accident. There is a substantial compounding of human errors.

[7] Values shown in parentheses account for the percent change in error being a contributing factor to the casualty event with the implementation of tug support for tanker transits.

12

Bligh Reef Dead Ahead: The Grounding of the Exxon Valdez

KARLENE H. ROBERTS
University of California, Berkeley

WILLIAM H. MOORE
University of California, Berkeley

For biographical information about Karlene H. Roberts, see page 1.

For biographical information about William H. Moore, see page 199.

The authors thank various members of the United States Coast Guard and the Exxon Shipping Company for their help and informative comments. We also thank Walter Parker and Edward Wenk, Alaska Oil Spills Commission; and William Shrenk, Natural Resources Defense Council.

Like Meyer and Starbuck, Hirschhorn, and Weick's contributions to this volume, this chapter tells a story of organizational failure. It is an unfolding analysis of management processes operating with pilotage, at the Coast Guard, aboard the *Exxon Valdez*, and in the Exxon Shipping Company before and at the time of the *Exxon Valdez* misfortune. The analysis is based on a review of the literature and on numerous interviews with marine industry experts. While much discussion of the grounding has focused on crew activities prior to and during the accident, it is generally agreed that the mishap was the result of a number of forces coming together in a disastrous way just after midnight on March 24, 1989. The ship's course is diagrammed in Figure 12-1.

When the *Exxon Valdez* hit Bligh Reef, the vessel was holed in eight of eleven cargo compartments and two ballast tanks. Most of the cargo loss occurred during the first eight hours after the grounding. Thirty minutes after the grounding, 115,000 of the ship's 1,263,000 barrels were lost. A total of 258,000 barrels, or eleven million gallons, were lost in all.[1]

Ironically just three months before this accident, the only other major spill in the 12 years of the Trans-Alaska Pipeline operation occurred when the *Thompson Pass* released 1700 barrels of oil. More than 8800 successful oil shipments had passed through Prince William Sound (PWS) without serious incident by March 24, 1989 (Alaska Oil Spill Commission, personal communication).[2]

One of the requirements of the Trans-Alaska Pipeline Authorization Act (TAPS) of 1973 was to establish and operate a Vessel Traffic Service (VTS) for PWS. The PWS VTS was the only federally mandated VTS in the country. The Port and Tanker Safety Act of 1978 authorized operations, surveillance and communication, routing systems, and fairways for supervising vessels in transit, and gave the Coast Guard the authority to establish routing schemes and specific times of entry, movement, and departure.

Unlike other VTSs across the country, Valdez VTS personnel could be utilized in non-VTS duties at the discretion of the Commanding Officer (CO). In a letter to the CO of the U.S. Coast Guard (USCG) headquarters in 1985, he stated, "What MSO [Marine Safety Office] Valdez does is much larger than just having a few people watch radar screens in the least-trafficked, yet fully federally mandated, VTS in the country." Watchstanding was reduced at the same time that the potential for problems due to ice floes in the sound increased. Procedures for certain eventualities were not well spelled out, or if they were spelled out were not implemented.

The VTS consisted of a Vessel Traffic Center (VTC), a radar surveillance system, and a communication system. The VTC was manned 24 hours around

[1] This information is from the National Transportation Safety Board (NTSB) report. However, L. Z. Katcharian, Marine Accident Investigator for the Marine Accident Division of the NTSB, provided the following figures in his report to the NTSB, dated May 8, 1989. "The vessel lost about 250,000 barrels (10,400,000 gallons) of its 1,264,164 barrels (53,094,510 gallons) of cargo of North Slope crude oil.

[2] Two to three major ships pass into and out of PWS daily.

the clock by two watchstanders (one radar watchstander and one radio watchstander). The radar watchstanders' responsibilities were to maintain vessel positions, while the radio watchstanders established and monitored radio contact for PWS. The radar surveillance system had initially been able to maintain contact with vessels from Port Valdez to areas south of Bligh Reef. Three hours before entering PWS, vessels were required to give VTS general information about vessel name, position, estimated time of arrival (ETA) to navigation in the VTS area, speed, cargo type, towing assistance, vessel impairments, and additional requested information. Once in VTS waters, vessels were required to report at various reporting points, and when changing speed and crossing and clearing the Traffic Separation Scheme (TSS).

The VTS was reorganized in 1982, making four of the five watch supervisors department heads who had little to do with supervising watches. In 1986, the CO of MSO Valdez proposed that the Marine Safety Office be downgraded to the Marine Safety Detachment (MSD). The proposal eliminated five VTS officer watchstander billets. In 1987 the watches were discontinued and replaced by a Command Duty Officer (CDO) or Officer of the Day (OOD). The CDO was not required to be at the VTS during routine vessel transits.[3]

In 1988 the VTS lost five billets. As a result, remaining personnel took on additional functions that had little to do with VTS, and by default the senior watchstander became responsible for supervising the day-to-day operations of the VTS. This person worked days and stood watches when anyone called in sick. Several of the OODs were enlisted personnel, junior to the civilian watchstanders they supervised. On the day of the accident only one OOD was a qualified watchstander. The station OOD on duty prior to the accident had never qualified as a watchstander. Reduction in personnel may have caused communication between the VTC and senior MSO/VTS personnel to decline. No officer's primary duty was to be in charge of the VTS.

Despite the fact that ships regularly deviated from the TSS, the CO of MSO Valdez reported to the National Transportation and Safety Board (NTSB) (Woody, 1989) that if a vessel knew its position and was maneuvering, no further radio contact was required. He continued, "There is no good reason for a ship to deviate from the TSS; a vessel requesting deviation is requesting something out of the norm." VTC watchstanders do not have the authority to allow vessels to leave the lanes, and if a vessel requests deviation the request is forwarded to the Operations Officer (OO) who forwards it to the CO or Executive Officer (XO) for a reply. Neither the CO nor the OO appeared to be aware that vessels regularly departed the TSS

In 1980, after the *Prince William Sound* lost power in the Sound, the Coast Guard recommended installing reinforced tow lines on tankers and requiring tugboats to escort them to Hinchinbrook Island. The lines were in-

[3] However, it was required that he be contacted in the event that vessels deviated from the TSS. The CDO could be contacted 24 hours a day if conditions arose in which vessels needed to deviate from the traffic scheme.

stalled. In 1981, James Woodle, the CO of Valdez, recommended that the Coast Guard radar system be improved in response to the break up of the Columbia Glacier (Davidson, 1990). Nothing was done. According to the NTSB Report (Woody, 1989) in 1984 the Coast Guard requested the installation of an additional radar site on either Glacier or Bligh Island. In 1984, the Coast Guard and oil companies met to talk about the increasing ice. In neither case was anything done. For a time the oil companies ordered their vessels to operate at reduced speed or only during daylight. In 1986, the Coast Guard issued a series of recommendations and directives that made pilotage so complicated that no one knew what was required (Davidson, 1990, p. 72).

A study done after the accident showed that the existing radar was incapable of reliable radar coverage of Valdez Arm. The number one (master) radar that synthetically displayed the TSS boundary lines was burned out. The Coast Guard was warned in 1984 that the system would begin deteriorating in the next two years without attention. After the accident, the OO testified that he noted its deterioration over the last two years. The contractor did not keep the system well maintained, and as a result it was inoperable up to 28 percent of the time. Between 1981 and 1984, 18.9 percent of the vessels transiting the VTS area deviated from the TSS because of ice.[4]

The *Exxon Valdez*'s bridge complement consisted of four deck officers (captain, chief mate, second mate, and third mate), and two able bodied seamen (ABs, one a helmsman and the other a lookout). The mates and able bodied seamen stood two four-hour watches each day with eight hours off in between. The day before the accident, Captain Hazelwood was off the ship while it was loading crude oil in Valdez. By his own confirmation he was drinking that day. The NTSB report (Woody, 1989) states that extrapolating from a blood test taken ten hours after the accident, his blood alcohol level would have had to be approximately 0.285 at the time he boarded the ship. A person boarding the ship this inebriated would have shown some evidence of physical impairment or would have needed some assistance. Additionally, a cab driver and an Alyeska (oil-company consortium) guard interviewed by the Board investigators reported that none of the *Exxon Valdez* crew members returning to the vessel were "under the influence of alcohol." According to Keeble (1991), no one on the ship observed any deficiency in Captain Hazelwood's behavior. The blood alcohol test gave a reading of 0.061, or a little more than over half of the drunk driving limit of 1.0 in Alaska and 50 percent higher than the 0.04 percent limit set by the Coast Guard for seamen operating ships.

[4] In August 1984, a meeting was called of operators, Coast Guard, state pilots, and Alyeska to discuss ice conditions. A Coast Guard representative mentioned their concern for ice conditions in PWS, though representatives at the meeting tried to downplay the problem (NTSB Factual Reports—Ice Conditions, p. 226). An Exxon representative said he was confident of the abilities of the masters of their vessels to handle the situation and would like to see operations continue as they were. An Arco representative agreed, saying he believed in preliminary planning reports but saw no need for further controls. Pilots concurred that masters would not transit if they felt the ice was too dangerous.

The ship left port at 2054. Federal and Alaska state law require that ships be under the control of a federally licensed pilot when transiting in U.S. pilotage waters (inside the three-mile territorial seas). In 1977, the state pilot association established a pilot station at Cape Hinchinbrook, using a converted fishing vessel, the *Blue Moon*. In 1980 the *Blue Moon* foundered. Due to the dangers involved in embarking and disembarking pilots in the outer Prince William Sound, the pilot station was moved to Rocky Point at Valdez Arm. The Alaska Board of Marine Pilots eliminated the state requirement for state pilotage between Cape Hinchinbrook and the pilot station at Rocky Point. The Federal Pilotage requirements still were in effect, though there were no transport pilots between Cape Hinchinbrook and Rocky Point. This created few problems since most trade masters held federal pilotage between Cape Hinchinbrook and Rocky Point.

In June 1985, proposed changes in pilotage regulations were introduced. The Coast Guard reduced the areas of required pilotage. In September 1986, the Coast Guard began to issue requests for pilotage on a case-by-case basis for tank vessel masters without pilotage endorsements. The major change was in the requirement of two-mile visibility in the sound with potential reassessment of this proposal during adverse weather conditions. The night of the *Exxon Valdez* accident a state pilot was aboard the ship until it reached Rocky Point. During the time he was aboard, Captain Hazelwood was off the bridge for approximately one hour and thirty five minutes. The pilot smelled alcohol on his breath.

Captain Hazelwood decided to take the ship out of the outgoing TSS and into the incoming TSS to avoid ice.[5] This was not an unusual course, and Hazelwood informed the Coast Guard that he was making this deviation. Only a short time before, the *Arco Juneau* had taken a similar course out of the Sound. Sylvia Gil and John Rush were the first to see *Exxon Valdez* on Bligh Reef. Their house at Ellamar overlooks Bligh Reef. According to John Rush, "Actually . . . there was no surprise to it whatsoever. We knew it was a question of time. They've been cutting that corner for years." (Keeble, 1991, p. 162) One speculation is that by cutting the corner out of the sound, tankers could cut a half hour from their exit time and perhaps four hours from their sailing time.

Shortly prior to his relief at 2355, the helmsman responded to an order from the master to sail the ship 180 degrees and put it on automatic pilot. Helmsman Harry Claar was puzzled by this order. He didn't check it with the master. The third mate was unaware that the ship was on automatic pilot. For the captain to put the ship on automatic pilot in confined waters and not tell the third mate was inconsistent with normal practice. The master left the bridge but not before asking the third mate, Gregory Cousins, if he felt comfortable

[5] This decision was probably made to increase reliable performance. Often decision makers are unable or unwilling to examine the unintended unsafe consequences of decisions made with the goal of increasing safety.

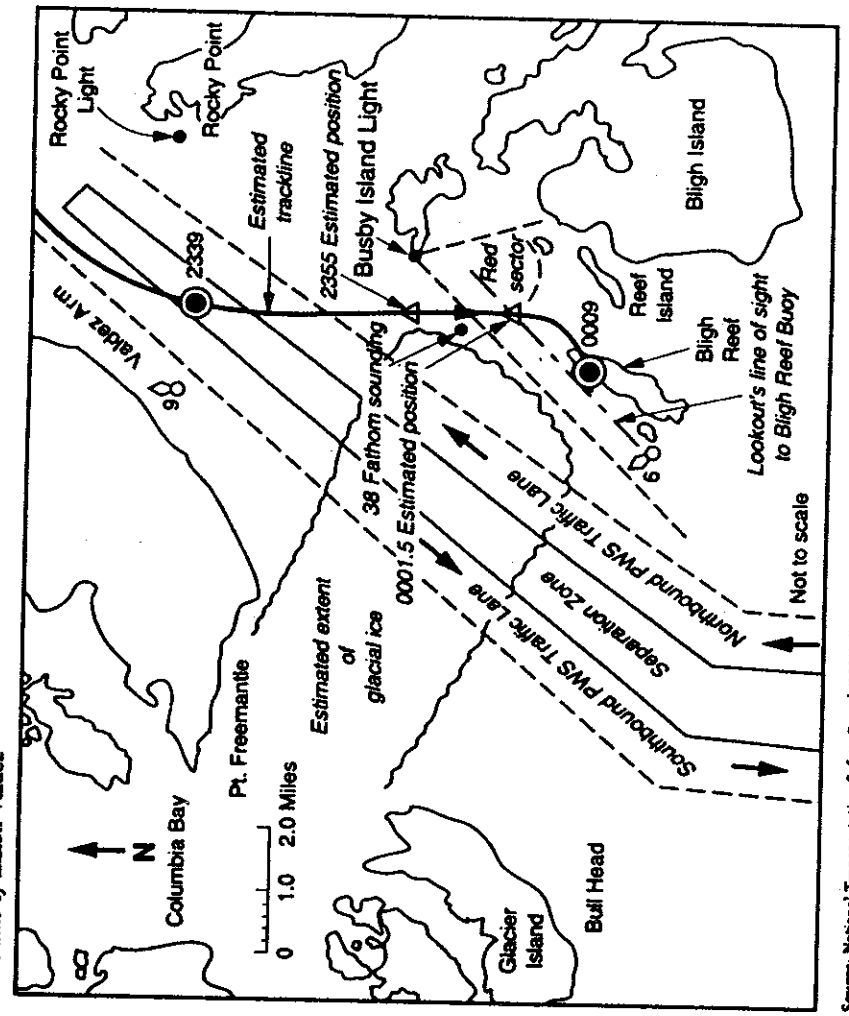


Figure 12-1
Trackline of Exxon Valdez

Source: National Transportation Safety Board (1990): "Grounding of the U.S. Tankship *Exxon-Valdez* on Bligh Reef, Prince William Sound, near Valdez, Alaska, March 24, 1989." PB90-916405 MTSB/Mar-90/04.

sailing the ship under these conditions. Cousins replied that he did. The master left the bridge at 2352.

At 2347, the ship left the outbound (TSS) going into the inbound lane to avoid the ice. At 2355, the helmsman was relieved by Robert Kagan (Davidson, 1990). The ship was on "load program up," which meant it was increasing its speed while exiting the harbor. One account has it that the *Exxon Valdez* was traveling at 12 knots and on automatic pilot just prior to hitting Bligh Reef (Davidson, 1990).[6] At his relief, the helmsman reported to the third mate that the ship was on automatic pilot. The third mate did not discuss the reason for the automatic pilot with the master. Keeble (1990) states that Cousins took the ship off automatic pilot when Kagan relieved Claar as helmsman.

At 2355, the third mate plotted the ship as 1.1 miles from Busby Island. Before midnight, the AB reported to the third mate a red light flashing every five seconds on the starboard side of the ship.[7] Kagan acknowledged this and stated he knew the light to be Bligh Reef, Light 6. The third mate ordered a right ten degree rudder, but the vessel did not move to this position. There was a six-minute delay before the third mate and helmsman responded to the fact that the ship did not begin to turn.

> The frequent fixing of the vessel's position could have taken a substantial amount of the third mate's time and would have limited his ability to concentrate on other important functions, such as watching for ice and conning the vessel. Conning also requires careful supervision of the helmsman. Under normal conditions, when a master or a pilot is conning a vessel, the watch officer assists by carefully observing the actions of the helmsman in response to orders from the master or pilot. This enables the officer conning the vessel to concentrate on observing and directing the vessel's movements. In this instance, the helmsman had limited steering experience and required additional supervision. The master was aware of the helmsman's limitations and should have considered them before leaving the bridge (National Transportation Research Board, 1989, p. 115).

Watch Condition C (Exxon Bridge Organizational Manual) states that two officers must be on the bridge during this transit. The third mate testified that normally two officers served on the navigation watch when Exxon vessels were maneuvering in confined or congested waters.[7]

About this time, the AB reported the light flashing every four seconds. The third mate ordered a right twenty-degree rudder. Moving at twelve knots while the ship was still engaged in maneuvering evolutions to avoid ice violated

---

[6] According to Keeble (1990), this ship maneuvers best at eleven knots. According to Exxon Shipping Company, sea speed for this ship is sixteen knots.

[7] All mariners know the phrase *red light returning*. It means always keep red buoys and red markers on the right when returning to port, and keep them on the left when departing. There is an exception to this. At a given point a ship might find a red light on its right, by virtue of its distance and angle from the marker.

prudent ship handling practices while it increased the risk of damage to the ship if an ice floe had been struck. Cousins then ordered a hard right rudder.

When the ship hit the reef, the third mate ordered a hard left rudder to get the vessel to stop swinging to the right and prevent the stern from swinging around. The ship had clearly skidded into Bligh Reef. The helmsman was confused about some aspects of the situation. According to Keeble (1991), when testifying at the master's trial the helmsman "would blurt out almost endearingly, 'I get so confused.' " (p. 41) He also reported that the third mate was panicky. The chief engineer stopped the engines at 0020. It is not clear from the NTSB report what time the ship hit the reef. According to Keeble (1991), it was probably eleven or twelve minutes after midnight.

Kagan obtained the unrated Able Bodied Seaman (AB) rating in 1981. Since that time, however, he had worked about seven and a half months documented time as an AB. He worked primarily as an ordinary seaman in unrated positions. No performance appraisals referred to an AB specific job. In 1986, the performance evaluator noted severe deficiencies in his ship handling skills. None of the performance evaluations were good.

The third mate held a second mate's license and first sailed as the third mate on an Exxon tanker in January 1987. He had sailed on five tank vessels owned by the company and had been employed by Exxon for nine years. According to Davidson (1990), he had completed approximately eighteen voyages in and out of Valdez, sailing in both unlicensed and licensed categories. At the time of the grounding, he had approximately 199 days of at-sea experience as a third mate. According to Keeble, Cousins made the passage through Prince William Sound twenty-six to thirty times, three of them on the *Exxon Valdez*.

The night before, Cousins slept from 0100 to 0720; after lunch he took a cat nap (1300 to 1350), relieved the chief mate for supper, and worked through to the grounding. The situation is further complicated because the chief mate had worked the entire time of the loading, was asleep, and was unavailable as an additional resource.

The third mate decided not to call his relief, the chief mate, until after they cleared the ice.[6] The third mate determined there was 0.9 mile between Busby Island and the ice floe and felt he could pass around the ice. He relied considerably on the radar, but did not correlate radar information with the navigation charts through position fixing. The submerged reef was not displayed on the radar.

The lack of vigilance with which the VTS handled operations the night of the accident is another factor behind the misfortune. Only one civilian watchstander and one enlisted radioman were on duty. But the accountability and

[6] The error might have been detected through the watch relief procedures. However, Keeble (1991) noted that crew members were attempting to help each other out by standing longer watches so their co-workers could get some sleep. Captain Hazelwood, himself, planned to take an extra watch.

responsibility rested with people who were not there. Neither the CO nor the XO were at the VTS. The VTC manual requires the watchstander to advise the OOD when a vessel deviates due to ice in the lanes. The 1600 to 2400 watchstander failed to do this. He said he believed the radar did not detect the *Exxon Valdez* because the radar was not working properly. However, he did not report a malfunction to his relief or to the electronics technician on duty. The watchstander's relief came on at 2333.

Thus, both the VTS and *Exxon Valdez* watches changed at approximately the same time. Neither watchstander knew that the *Exxon Valdez* had altered course from 200 degrees to 180 degrees. The *Exxon Valdez* was lost on the radar but could have been picked up. The 0000–0800 watchstander said he did not try to do this because he had been told by the other watchstander that the *Exxon Valdez* was no longer visible on radar. At the time of the accident, the watchstander was away getting a cup of coffee. That the radar was operating appropriately is evidenced by the fact that the watchstander had no difficulty detecting the grounded ship.

The ship previously leaving the port reported heavy ice to the VTS, but the VTS saw no reason to report this to the *Exxon Valdez* or to more carefully monitor it. At about 1930, a passenger ship approached Valdez. Its captain said the ice was some of the worst he had ever seen, and he reduced speed. He did not report this to the VTS. At 1930, the outbound *Arco Juneau* reported ice in the TSS. The VTC operator said he was concerned about the heavy ice reported by the *Arco Juneau*, but that factor did not motivate him to have the ship report its position more frequently, nor did he report that to the *Exxon Valdez*. Both ships transited during the day and neither had as far outside the TSS to go as the *Exxon Valdez* because when the latter ship transited, the ice was much further to the northeast.

The *Exxon Valdez* remained on course 180 degrees for nearly 18 minutes. The VTC operator had ample time to call the vessel and ascertain its intentions. Any inquiry from the VTC regarding the vessel's intentions probably would have alerted the third mate to turn earlier or apply more rudder. The VTS communication system failed to meet the Coast Guard's requirement of 99.9 percent operational status. During the event of March 23, the Naked Island and Cape Hinchinbrook remote communication sites were inoperable. The system was old, requests for money had been denied, and the harsh Alaskan climate degrades the system easily. At 0027, the master let the VTS know the ship had run aground. Only then did the VTS watchstander know it had gone aground. He then adjusted the radar and picked up this information.

At 0035, the master ordered the main engine restarted. According to Keeble (1991), he gave the following orders: "Half ahead, full ahead, slow ahead, dead slow ahead, stop." A number of accounts stated that he tried to get the ship off the reef, which might have resulted in its capsizing. These orders are inconsistent with that theory. According to Keeble (1990), the captain stabilized the ship and protected his crew, and his actions were the best that

could possibly have been taken. According to NTSB documentation, the record fully supports the fact that had the master gotten the ship off the reef it would have capsized. Other evidence suggests it might not have (Brady, 1960).

Chief Mate Kunkel was awakened by the grounding. He went to the cargo control room to assess damage. He determined that the stress on the ship exceeded acceptable limits and took this information to the master, arriving on the bridge at 0030 or 0035. Between 0035 and 0100, Kunkel performed further analyses and concluded that if the vessel were not supported by the reef it would capsize. He relayed this information to the master. At 0107, the master was still advising the Coast Guard that the ship's stability was acceptable. At 0141, the engine was shut down.

Some of Exxon's policies contributed to the accident, while others were efforts to avoid such accidents. Two federal statutes cover Exxon's behavior. One says that an officer cannot take charge of the deck watch on a vessel when leaving a port unless he has been off duty for at least six of the twelve hours immediately before leaving. Another statute says a licensed individual or seaman is not required to work more than eight hours a day except for safety related functions.[9] Apparently Exxon had no provision for giving six hours of rest to any deck officer before getting underway.

Manning schedules were conceived when tankers were making longer journeys, thus allowing sea time for both maintenance and catching up on rest. Crew member tours were lengthened from sixty to ninety days. During 1988's senior officer's conferences, Exxon management discussed demanning with senior officers. It was recognized that a growing number of companies operated their vessels with significantly fewer personnel than Exxon. Exxon provided data to the NTSB that reduced manning was associated with better, not poorer crew performance. More recent study shows no negative impact on safety by demanning practices within the maritime industry (National Research Council, 1990).

Exxon stated, "It is our conclusion that, when addressing improved safety performance, management focus, leadership and effective supervision are more critical elements than crew size." In 1986, the company instituted a safety initiative: "As part of this effort, management teams, frequently accompanied by officials of the unlicensed union, visited every ship in the fleet to train personnel in new safety concepts. This was supplemented by one full day of safety training provided to all senior officers during each of the next two fleet management conferences. . . ."

However, there is no evidence that Exxon had policies or procedures to compensate for the risks of using smaller crews. No supervisory training recognized such factors as tiredness, social isolation, longer hours at sea, and so on. There was no company program to monitor officer's work in excess of eight

[9] The average workday is about ten hours, which includes voluntary overtime.

hours a day. There is evidence that officers do deck work that unlicensed workers did previously. Exxon continued to increase crew work load after the accident, and plans to further reduce crew size and to lower qualifications.

The policies Exxon had in updating fleet and reducing crew were consistent with those of the industry. Exxon's Seaman's Union officers expressed concern that maintenance was regularly deferred on the ships because of insufficient manning levels and because of Exxon's attempt to convince the Coast Guard that existing manning levels included too many crew by not authorizing overtime.

In June 1988, Frank Iarossi (then president of Exxon Shipping Company) presented a paper titled "Surrendering the Memories" in which he stated that it was Exxon's policy to reduce its standard crew compliment to sixteen by 1990. He noted that other ships (mostly foreign flag) successfully operated at such levels. The paper makes little mention of considerations of ship safety and crew fatigue, and it focuses solely on economic issues. The NTSB came to possess three memos to Exxon Shipping Company masters ordering them to reduce overtime purposefully to satisfy Coast Guard overtime concerns and to argue better for reducing manning levels.

The company's written policies about alcohol and drug abuse were not taken very seriously. The policy instructed supervisors to report to the medical department employees whose performance was unsatisfactory due to alcohol use. Crew members were not to perform job duties within four hours of having a drink. Hazelwood entered an alcohol rehabilitation program in 1985; the company learned about this when his supervisor tried to contact him. No supervision was involved in making sure that he continued with some sort of support group. The NTSB concluded that Hazelwood should have been confined to shore duty until there was ample proof that this problem was under control. His performance evaluation of 1988 was more than satisfactory.

Exxon had fleet managers and port captains (later, ship group coordinators) who monitored Hazelwood in port. It was stated that Hazelwood was also monitored at social functions. The company was unaware of the revocation of his driver's license in 1985 and 1988. No attempt was made by the Exxon personnel to visit Hazelwood when he was in Valdez. The company had alcohol testing equipment aboard the *Exxon Valdez* but had no indication the master had been drinking. Hence, no testing was ordered.

Exxon's performance appraisal system appeared to leave something to be desired. Annual performance appraisals for the master are not available for every year. The company made no statement about how it follows up on appraisals. Are they only done for salary increases or are they done as part of a larger performance improvement effort? Does anyone provide feedback to the person evaluated? A number of statements about Hazelwood's performance lead to the conclusion that he had difficulties managing people. These difficulties emerged as early as 1974 (NTSB). One could ignore one or two such statements, but they appear repeatedly through the years.

OVERALL ANALYSIS

In general, the *Exxon Valdez* collision looks like a story of organizational atrophy (system entropy) over time. The pilots reduced piloting requirements, the ship operated with two few officers on the bridge, and the Coast Guard had reduced force in the VTS over the years. While the accident lends itself to analysis along many different lines (e.g., failure to recognize the importance of the interdependent nature of organizations simultaneously working with complex technologies, lack of on-line information processing with real time feedback, and so forth), we highlight only three issues here: the operational culture of the participating organizations, training, and requisite complexity.

Culture

The culture of any organization is often subtle and often operates just below the surface of the everyday consciousness of its employees. As pointed out by Koch (this volume), organizations in which safe operations are mandatory in the prevention of behaviors with catastrophic consequences must develop cultures in which sensitivity to safety awareness and safety issues is paramount. It appears that the state pilots, the Coast Guard, and the Exxon Shipping Company were all characterized by weak cultures with regard to safety. Schulman (this volume) describes how safety-related interactions and behaviors are constantly renegotiated in a high-reliability organization. Over time, any organization moves to states of lesser organization unless this occurs.

In this situation, such renegotiations failed to occur. Over time, the pilots had reduced pilotage requirements for PWS, and there did not appear to be agreed-upon procedures for a pilot to engage in when he confronted a master who had been drinking. Pilot associations could develop standard procedures for such an event (including reporting it to the Coast Guard and the shipping company). The relationship established between pilots and masters since the days of Henry VIII does not favor such activity and should be re-examined.

The same weak culture with regard to safety appeared on both the *Exxon Valdez* and in the Exxon Shipping Company. In hindsight, one can say that the *Thompson Pass* incident three months earlier should have acted as a wake-up call. Such a response could prevent worse accidents in the future. The U.S. Navy exhibited this kind of response with its one-day standdown to focus on safety in 1989 after the occurrence of five serious accidents in a very short period of time. While that standdown may have been largely politically driven, it no doubt focused attention on safety for Navy personnel.

Greater attention to safety, at the possible expense of profit, would have been difficult to obtain at Exxon. First, the most serious accident the oil industry had previously incurred was the *Amaco Cadiz* spill in March 1978, a considerably less costly misfortune. That, in itself, likely influenced management's perception of the seriousness of tanker spills and influenced what it felt it had to be ready to deal with.

Second, the company, indeed the maritime industry, is in the grips of discussion about demanning. Demanning poses a tension against building in redundancies that can spot and prevent some kinds of catastrophes. When an organization suspects that the nature of error in it is such that the next error may be the last trial in a trial-and-error sequence, it engages in activities to avoid error, one of which is usually redundancy. If one has redundancy in observation and thinking, one can rely less on constraining written procedures and more on local expertise. Some organizations require high degrees of both, such as the nuclear power plant discussed by Schulman (this volume).

Another aspect of the culture is the development of corporate and operational goals that are synchronous with regard to maintaining safety. A situation in which bridge watchstanders are rewarded (if only in terms of having their buddies similarly help them later) for standing longer watches and helping shipmates get additional sleep is possibly consistent with a profit goal and is inconsistent with a safety goal. The goal of an alcohol-free culture is inconsistent with lackadaisical compliance procedures. Cultures take a long time to build (Schein, 1990; Trice and Beyer, 1984) and organizations that suddenly can become volatile need to think about what they have built and whether their cultures are sufficient for the safety task.

The Coast Guard culture, too, seems to have shifted over the years. Perhaps the years of refusals of requests to replace and repair equipment alone were enough to send a strong message to the Valdez VTS about the Coast Guard's and maybe its financial underwriter's (the Congress) expectations of its operations. When staffs are reduced and equipment is allowed to deteriorate, employees cannot avoid having the feeling that they and their mission do not have top priority. Allowing shift changes at the same time as they occurred in the organizations the VTS serviced, and having personnel with authority and responsibility for deviations in the TSS completely unhooked from the TSS decision-making process, are two examples of a system that can only respond to a potential disaster with a loose confederation.

Training

Training is an issue closely related to culture and is often used to stamp into employees the desired culture of an organization. The first aspect of the *Exxon Valdez* situation that strikes one is the apparent overall lack of emergency simulations or drills. Drills must include all parties so that in the event of a true surprise (and surprises will always happen) the parties will have worked out the relationships among themselves. Such drills must be conducted frequently enough so that turnover across the organizations does not erase all organizational memory, and so that new responses can be devised for changing technologies and environmental circumstances.

Though not a perfect model, one potential prototype is followed by some nuclear power plants. Every two years, the Pacific Gas and Electric Company (PG&E) conducts a full-scale drill for a problem at its nuclear power plant at

Diablo Canyon in California. Representatives from state agencies, the parent company, Diablo Canyon, the city of San Luis Obispo, local fire departments, and others participate. Each time the drill is conducted, a different scenario is presented. In many respects no simulation can appropriately map an accident because a day has to be decided upon to conduct the drill, and adrenalin may not be flowing. However, people play their own roles from the locations in which they would be at the time of an accident (i.e., San Francisco, Diablo Canyon, Sacramento, etc.). This procedure at least recognizes the importance of agency interdependence in case of an accident. When asked why such drills are not conducted more frequently, company representatives state that the cost is prohibitive.

Participation in such a drill is one way to ascertain an approximate hierarchy across agencies for decision making and control. In drills, players can work these things out, and they may discover what information, authority, responsibility, and materials they lack in order to do their jobs in an emergency.

As well as being a device to work out relationships, simulation is about the only kind of training that simultaneously involves all possible participants in emergency responses. Following simulations, written training materials can be sent to all participants. While our analysis here only includes the Coast Guard, the pilots, and the Exxon Shipping Company, in reality the situation included many more players who should also be included in simulation training. In this situation, we see no evidence of training in emergency response.

While system-wide training is important, so, too, is individual training. Here, if the Coast Guard thought it was important for watchstanders to check on traffic frequently, to keep records of traffic moving into and out of the TSS, and so on, it either failed to train or to motivate the watchstanders to do so. Similarly, while the Exxon Shipping Company stated that leadership and supervision were more important than crew size in maintaining safe operations, and indicated that it trained crews aboard its ships, either the training was insufficient, or inappropriate motivators produced the conditions that led to the events of March 24. Performance evaluations are often used to identify training needs. In this case, it was noted that Hazelwood had some difficulties managing people. These difficulties might have been corrected with appropriate training. The helmsman also had deficiencies in doing his job and had been assigned mostly nonrated jobs by the company. The combination of few redundancies and skills deficiencies on the bridge contributed to the situation.

Requisite Complexity[10]

Perrow (1984) discusses tight coupling as a major factor in "normal accidents." Normal accidents are events brought on in systems by tight coupling and complex interactions that cause enormous damage. Perrow discusses the importance of tight coupling in creating such accidents. Here it appears we have a disaster *without* tight coupling and complex interactions. Weick (1987) discusses the importance of the requisite variety of an organization matching the requisite variety of its environment in highly reliable organizations. This appears to be a situation in which the requisite variety of the organizations involved did not match the requisite variety of the situation that required managing.

Both the shiphandling requirements and the nature of the environment prescribed the use of a more tightly coupled system in which players in various organizations recognize their interdependence with one another. An underelaborated mechanistic, nondifferentiated system; rather than a fluid, changing, organic, organizational system; was put in place to respond to a fluid, unstable, and complex environment (Burns and Stalker, 1961).

The ship's crew were only loosely coupled with one another. The master was away from the bridge when the accident happened and the three watchstanders on the bridge were only loosely interconnected. Tight interconnections would have been represented by continuous feedback and checking with one another about the meaning of orders, placement of warning lights, and other factors.

The ship's crew was only loosely connected with the pilot, who apparently spotted a danger signal and failed to raise a question about it on the ship. The pilot, the Coast Guard, and the Exxon Shipping Company were also only loosely, if at all, connected with one another.

Coast Guard officers and watchstanders were only loosely connected with one another, as evidenced by the fact that the people with authority and accountability for ship activities were not at the VTS, and the two watchstanders at the VTS and their shift replacements did not exchange important information about ship traffic and ice floe conditions. A further disconnect took place when one watchstander left the VTS to get coffee at the time of the accident.

Exxon Shipping Company policies, too, were in a state of disconnect. Its drug and alcohol policies were apparently only casually monitored. The company's performance appraisal system appeared to be largely independent of how it managed employees. Whatever the training of shipboard personnel was seemed either largely disconnected from behavior, or perhaps reinforced the very behaviors that occurred on the bridge.

CONCLUSIONS

Many of the issues discussed in this volume are relevant when one must consider the prevention of accidents such as occurred to the *Exxon Valdez*. As indicated previously, both Koch (this volume) and Schulman (this volume) emphasize the development and nurturance of safety cultures in organizations in which errors can lead to catastrophic outcomes.

Organizations can apply the theoretical perspectives offered by Rochlin (this volume) and Creed et al. (this volume) in answering their own questions

[10]Our thanks to Karl Weick for his inputs to this section.

about the degree to which performance is guided by some underlying understanding of what the organization wishes to accomplish. Does the organization have a theory about what constitutes reliability (Rochlin), and about the appropriate way for it to view and improve its effectiveness (Creed et al.)?

It appears that linkages within and, surely, between organizations in this situation contributed to the accident. Hirschhorn (this volume) alerts us to the importance of building a system in which people can act in a healthy manner.

Foushee and Lauber (this volume), Weick (this volume), and Eisenhardt (this volume) all suggest that in addition to system characteristics, the cognitions, actions, and interactions of the organization's members must be examined and thought about. If people carry inappropriate cognitions (as perhaps the bridge team did), the probability is higher than an accident will occur than it is if they have correct mental representations of their situations (Weick and Daft, 1983). People perform best when the glue of social interaction plays a hefty role in their organizations (Schulman, this volume; Foushee and Lauber, this volume). Trusted counselors (Eisenhardt, this volume) may also play a key role in organizational action. Basically, pilots and VTSs are the trusted counselors of the maritime industry. However, they can only serve this role in a limited capacity, and in this case the VTS was absent from service.

As pointed out by Meyer and Starbuck (this volume), organizations' actions and inactions are heavily tied to their political systems. Management would do well to assess these systems carefully because it may be, as Creed et. al. speculate, that if technologically advanced organizations are to operate safely and reliably in uncertain environments, they must minimize political activity so the organization is not overwhelmed by political behavior when it needs to attend to potentially very damaging activities. In this case, it is impossible to know the degree to which political behaviors may have influenced field operations.

Finally, several basic research programs that model risk are alive and well in various industries (Bea and Moore, this volume; Paté-Cornell, 1990, among others). While such research is useful in identifying causal factors in accidents, one should not just complacently use the results of such work. Users need to think about whether the weight given various factors is appropriate to their situations and whether the models they use are sufficiently inclusive.

REFERENCES

Brady, E. M. (1960). *Marine Salvage Operations*. Centerville, MD: Cornell Maritime Press.

Burns, T., and G. M. Stalker (1961). *The Management of Innovation*. London: Tavistock.

Davidson, A. (1990). *In the Wake of the Exxon Valdez*. San Francisco: Sierra Club.

Keeble, J. (1991). *Out of the Channel: The Exxon Valdez Oil Spill in Prince William Sound*. New York: HarperCollins.

Davidson, A. (1990). *In the Wake of the Exxon Valdez*. San Francisco: Sierra Club.

Keeble, J. (1991). *Out of the Channel: The Exxon Valdez Oil Spill in Prince William Sound*. New York: HarperCollins.

National Research Council (1990). *Crew Size and Maritime Safety*. Washington, D.C.: National Academy Press.

National Transportation Research Board (1989). *Exxon Valdez Casualty Factual Reports*.

Paté-Cornell, M. E. (1990). "Organizational aspects of engineering system reliability: The case of offshore platforms." *Science, 250*, 1210–1217.

Perrow, C. (1984). *Normal Accidents: Living with High Risk Technologies*. New York: Basic Books.

Schein, E. H. (1990). "Organizational culture." *American Psychologist, 45*, 109–119.

Trice, H. M., and J. M. Beyer (1984). "Studying organizational culture through rites and ceremonials." *Academy of Management Review, 9*, 653–659.

Weick, K. E. (1987). "Organizational culture and high reliability." *California Management Review, 29*, 112–127.

Weick, K. E., and R. L. Daft (1983). "The effectiveness of interpretation system." In K. S. Cameron and D. A. Whetton (eds.), *Organizational Effectiveness: A Comparison of Multiple Models*. New York: Academic Press.

Woody, W. (1989). National Transportation Safety Board. *Grounding of the U.S. Tankship* Exxon Valdez *on Bligh Reef, Prince William Sound near Valdez, Alaska*. PB90-916405. Washington, D.C.: NTSB/MAR90/04.

Sutton, R. I. and P. L. Kahn (1987). "Prediction, understanding, and control as antidotes to organizational stress." In J. W. Lorsch (ed.), *Handbook of Organizational Behavior*. Englewood Cliffs, NJ: Prentice-Hall, 272–285.

Wagner, J. A. and M. K. Moch (1986). "Individualism collectivism: Concept and measure." *Group and Organization Studies, 11*: 280–304.

Weick, K. E. (1983). "Contradictions in a community of scholars: The cohesion-accuracy tradeoff." *The Review of Higher Education, 6*(4), 253–267.

——— (1988). "Enacted sensemaking in crisis situations." *Journal of Management Studies, 25*, 305–317.

Wood, R. E. (1986). "Task complexity: Definition of the construct." *Organizational Behavior and Human Performance, 37*, 60–82.

Zeleny, M. (1986). "The law of requisite variety: Is it applicable to human systems? *Human Systems Management, 6*, 269–271.

11

Operational Reliability and Marine Systems

ROBERT G. BEA
University of California, Berkeley

WILLIAM H. MOORE
University of California, Berkeley

Robert G. Bea is a professor in the Department of Naval Architecture and Offshore Engineering and the Department of Civil Engineering, University of California at Berkeley. He started his engineering career with the U.S. Army Corps of Engineers in 1955. He then worked for Shell Oil and Shell Development Companies for 20 years in a variety of engineering, construction, and research assignments around the world. He later became Vice-President and Chief Engineer of the Ocean Services Division of Woodward-Clyde Consultants. In 1980, he joined PMB Engineering (a Bechtel subsidiary) as a Senior International Consultant and Vice President. He was appointed to the faculty at Berkeley in 1989.

The authors recognize the insights, guidance, and leadership in this work provided by Professor Karlene Roberts of the Haas School of Business Administration at the University of California, Berkeley, and Professor M. Elisabeth Paté-Cornell of the Department of Industrial Engineering and Engineering Management, Stanford University. Key items of data and information for the work were provided by the Marine Investigation Group of the National Transportation Safety Board and by the Marine Safety Group of the U.S. Coast Guard.

The work is a result of research supported in part by NOAA, National Sea Grant College Program, Department of Commerce, grant #NA89AA-D-SG138, project #R/OE-17, through the California Sea Grant College, and in part by the California State Resources Agency. The U.S. government is authorized to reproduce and distribute for governmental purposes.

The work was also sponsored in part by Chevron Corporation, Chevron Shipping Company, Amoco Production Company and Amoco Transport Company, Unocal Corporation, the California State Lands Commission, and the U.S. Minerals Management Service. The support and guidance of these sponsors is gratefully acknowledged.

Professor Bea's interests in offshore platforms and pipelines, reliability methods, environmental forces, and marine foundations have resulted in publication of more than 150 papers. He is the author of a recently published book titled *Reliability Based Design Criteria for Coastal and Offshore Structures.* He has received a number of awards including the J. Hillis Miller Engineering Award, the American Society of Civil Engineers Croes Medal, and the Bechtel Fellow Award. He is a member of the National Academy of Engineering.

William H. Moore is a graduate research engineer pursuing a Doctor of Engineering degree with the Department of Naval Architecture and Offshore Engineering at the University of California at Berkeley. He has an M.S. degree in Ocean Systems Management from the Massachusetts Institute of Technology and a B.A. degree in Statistics from the University of California at Berkeley. His current topics of research are examining human factors in operations of tankers and offshore platforms, and he has research interests in ship operations, port planning and operations, and shipping economics.

The source of a majority of high-consequence accidents associated with marine systems such as offshore platforms and tankers can be attributed to compounded human and organizational errors (HOE) (Bea, 1989; Paté-Cornell & Bea, 1989). More than 80 percent of these accidents are founded in problems that develop primarily during operations of these systems. Recent examples include the *Occidental Piper Alpha* North Sea platform explosions and fire in 1988 (167 men killed), the *Odeco Ocean Ranger* capsizing off Newfoundland in 1982 (84 men killed), and the grounding of the *Exxon Valdez* off the coast of Alaska in 1989 (258,000 barrels of crude oil spilled).

Traditional engineering of marine systems focus primarily on structure and equipment. It aims to ensure that the proper amounts of structural materials are in place, that suitable functioning equipment is provided, and that the structure is constructible and serviceable for its intended purposes. Given that something in excess of 80 percent of the failures of these systems are the result of HOE, it is timely for engineers, managers, and regulators to begin formally addressing people and organizational considerations in design, construction, and operations of marine systems.

At the present time, there is no structured quantitative method to assist engineers in identifying and evaluating effective strategies either to design more human-error tolerant systems or to include consideration of the potential for human and organizational errors as an integral part of reliability improvement assessments. Those critical of the use of reliability-based methods in engineering marine systems cite the omission of consideration of the "human aspects" as a primary obstacle to their meaningful application (Reid, 1989).

This chapter discusses the impact of human and organizational error on the operational reliability of offshore platforms and tankers. It examines how

qualitative and quantitative probabilistic risk analyses can be used as a tool to help evaluate the impact of HOE and HOE management alternatives. Case histories based on several recent marine disasters are used to illustrate the insight developed as a result of such analysis.

MARINE SYSTEM RELATED HOE STUDY BACKGROUND

In 1989, after completing a reliability study for the *Occidental Piper Alpha* replacement platform *Piper Bravo*, the senior author and Professor Elisabeth Paté-Cornell initiated a cooperative year-long pilot project to develop a first-generation HOE-PRA analysis procedure. The procedure addressed errors involved in designing, constructing, and operating fixed offshore drilling and production platforms, with an emphasis on the organizational aspects and the design phase. The results of that work are summarized in Paté-Cornell and Bea (1989).

The authors have continued research to further develop and verify an HOE-PRA analysis procedure directed at marine structure *operations*, and specifically, at floating marine structures (tankers and floating drilling and production systems). The research addresses the interactions of four major elements: (1) the physical system (structure and equipment level), (2) the operating personnel (individual/s level), (3) the organization directly responsible for management of the operating personnel (company level), and (4) other organizations that are involved in and that influence the operations (societal level).

The approach used in this project is founded on five primary tasks, as follows.

Task 1. Identify, obtain, and analyze well-documented case histories of tanker and offshore platform accidents whose root causes are founded in HOE. Accident investigation reports by the U.S. Coast Guard, Minerals Management Service, and the National Transportation Safety Board, and information provided by U.S. ship and platform operators provide the majority of real-life case histories of operations-caused failures for this project. In addition, accident investigation reports by the Canadian Royal Commission (sinking of the *Ocean Ranger*), the U.K. Department of Energy (*Piper Alpha* fires and explosions), and the Norwegian Petroleum Directorate (*Alexander Kielland* sinking) are used to provide additional case histories.

Task 2. Develop an organizational and classification framework for systematically identifying and characterizing various types of human and organizational errors. Human-error organizational frameworks developed for operations of high reliability systems (e.g., aircraft, nuclear power plants) will be reviewed and applied as appropriate.

Task 3. Develop general analytical frameworks based on real-life case histories to characterize how the human and organizational errors interact to cause the accidents. It is anticipated that "influence diagrams" (Paté-Cornell and Bea, 1989; Bea, 1989) will provide the basic analytical frameworks.

Task 4. Formulate quantitive analyses for the case histories based on probabilistic risk analysis procedured using influence diagrams. Perform quantitative risk analyses to verify that the analyses can reproduce the results and implications from the case histories and general statistics of marine accidents. The real-life accident case histories used to create the analytical models will be different from the case histories used to test and verify the models.

Task 5. Investigate the effectiveness of various alternatives to reduce the incidence and effects of human and organizational errors. Evaluate the costs and benefits in terms of effectiveness of risk reductions (product of likelihoods and consequences). Case history-based evaluations of the alternatives and tradeoffs will be used to illustrate the processes associated with developing effective strategies for managing human and organizational errors in operations of tankers and offshore platforms.

This chapter summarizes some of the key observations, insights, and analytical procedures developed as a result of this work. They are based on findings from a large number of other researchers who have studied this problem for the last 10 years.[1]

There are two complimentary approaches to the evaluation and management of HOE in improving reliability: (1) *qualitative* and (2) *quantitative*. Both approaches have benefits; our work indicates that they both should be mobilized to identify how and where to improve HOE management. One approach (qualitative) can and should form the framework for the other (quantitative).

The structure and interactions of humans, organizations, and systems is very complex. Further, there is little definitive data to assist in the evaluation analysis of such problems. Data on human performance in different tasks under different constraints and environments are only beginning to be assembled.

Is what we have to work with ready for application? In the authors' opinions and experiences, the answer is a demonstrable yes! The principal objective of the explicit introduction of HOE considerations into conventional reliability analyses is to help identify potentially critical weaknesses in the human, organization, and systems that are designed, constructed, and operated, and then to give one a basis to evaluate and justify alternatives to improve the reliability of marine systems. Our record of marine safety attests to the fact that this must be done if the industry is to make major improvements in the reliability of its systems. It is the process of evaluation, assessment, analysis, and allocation of safety resources that can be dramatically improved with the present state of development in HOE reliability management procedures.

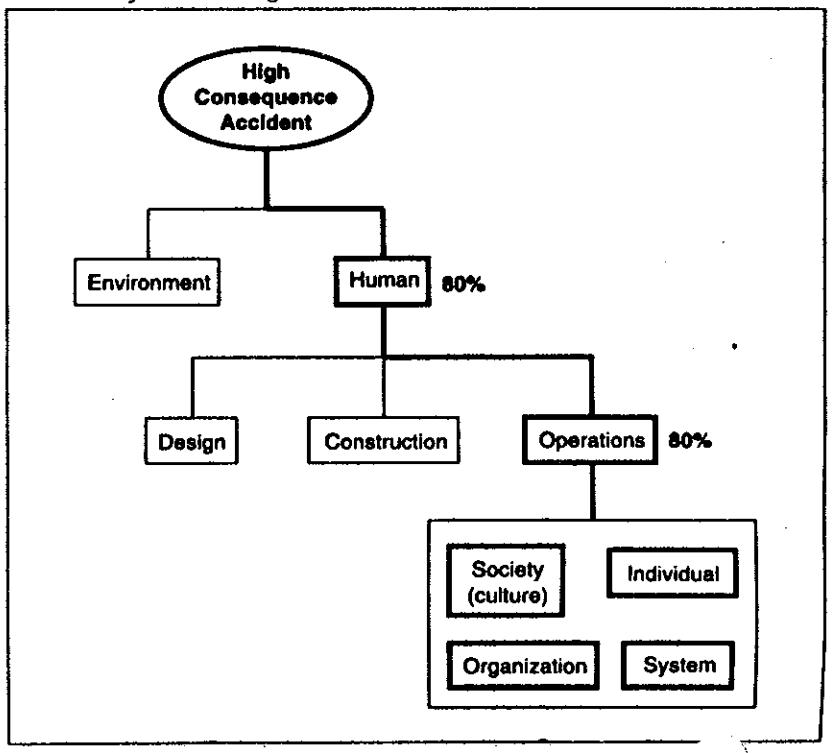
[1]The authors have been given significant directions and HOE data by a number of individuals and organizations with extensive backgrounds in marine safety, and in particular, the operations of HOE related aspects of safety. These include the U.S. Coast Guard, National Transportation Safety Board, Human Factors Group at NASA-Ames, and the High Reliability Organization Project at the University of California, Berkeley.

ACCIDENT ORIGINS

As shown in Figure 11-1, high-consequence accidents can be the result of a number of events. The first distinction is between *environmental* and *human factors*. Catastrophic accidents due to environmental factors can be the result of failures that exceed the "reasonable" demands of the structure during its lifetime. Two examples are experiencing the 1000-year wave event during the lifetime of a structure which has been designed for the 100-year wave event, or failure due to earthquake far in excess of the platform design capacity. These failures are unavoidable "acts of God."

High-consequence accidents resulting from human errors can be differentiated into those caused by *design*, *construction*, or *operations*. Accidents can be the result of improper design and construction of the system. For example, primary contributors to the capsizing of the *Alexander Kielland* (123 men killed)

Figure 11-1
Breakdown of Accident Origins



were the lack of redundancy (design) and cracks (construction) in the structure (Moan, 1981).

Accidents resulting from operations can be categorized into *societal* (cultural), *organizational*, *individual*, and *system* errors. Societal values can substantially influence the frequency of human and organizational errors. Expedient offshore development in the United Kingdom, resulting from the economic crises of the 1960s and 1970s, led to limited safety regulation and significantly high rates of marine accidents (Carson, 1982; Noreng, 1980).

Organizational factors have been shown to be associated with operational reliability for offshore platforms (Paté-Cornell and Bea, 1989; Paté-Cornell, 1990). For example, errors in management decisions resulted in the loss of the *Odeco Ocean Ranger* (Heising and Grenzebach, 1989; Royal Commission on the *Ocean Ranger* Marine Disaster, 1985) and the excessive loss of life aboard the drillship *Glomar Java Sea;* here 82 men were killed (National Transportation Safety Board, 1987).

Individual errors can also result in accidents. The chain of events that led to the *Occidental Piper Alpha* accident was initiated by events emanating from an unfinished maintenance job in the gas compression module (Lord Cullen Report, 1990; United Kingdom Department of Energy, 1988). Rochlin (this volume) provides extensive discussion of several ways human error can ramify into accidents.

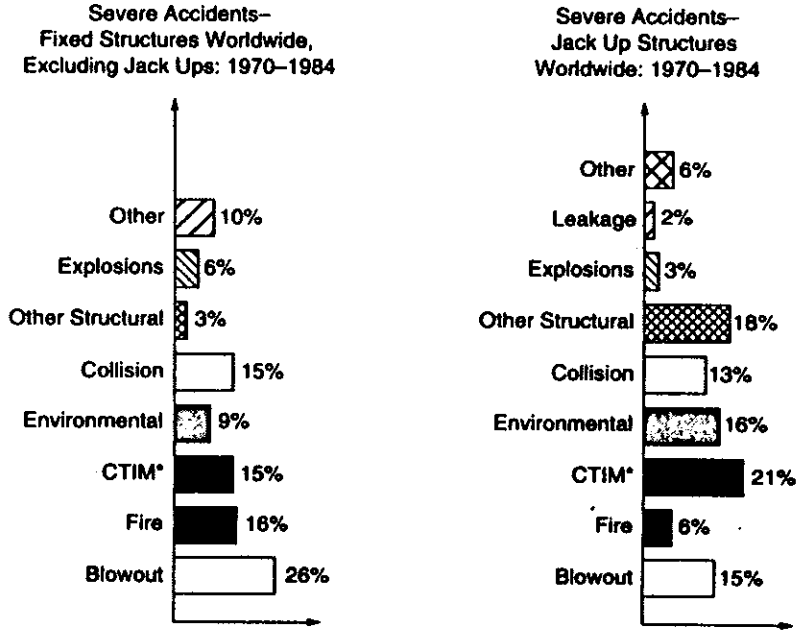
Errors that occur because of human–system (equipment, structure) interfacing are system errors. System errors can be attributed to design errors and may result in an operator making improper decisions. System errors led to the loss of the ballast control aboard the *Odeco Ocean Ranger* (Royal Commission on the *Ocean Ranger* Marine Disaster, 1985) and emergency system failure aboard the *Occidental Piper Alpha* (Lord Cullen Report, 1990; United Kingdom Department of Energy, 1988).

Errors can be further categorized into *active* and *latent* errors. Active errors are those that have an immediate effect on the system (usually errors by front-line operators), while latent errors surface only once the active errors have occurred; these are primarily organizational and system errors (Reason, 1990). For example, the inadequacies of Alyeska's oil spill contingency plans (latent errors) only became blatantly apparent once the *Exxon Valdez* ran aground on Bligh Reef (active errors). Because Alyeska (a consortium of oil companies) was so ill-prepared for a spill of this magnitude, it took 14 hours to initiate a response to the spill (Davidson, 1990).

HUMAN ERRORS

Human errors are the basic cause of failure in many engineered systems (Bea, 1989; Heising and Grenzebach, 1989; Melchers, 1987; Moan, 1983; Offshore Certification Bureau, 1988; Paté-Cornell and Bea, 1989; Veritec, 1988; Wenk, 1986). Figure 11-2 (Bea, 1989) summarizes the causes of severe accidents

Figure 11-2
Severe Offshore Accidents, 1970–1984



*Construction, Transportation, Installation & Mobilization

Source: Bea, 1989

involving fixed and mobile offshore structures used in the development of offshore hydrocarbons during the period 1970–1984 (Veritec, 1988). Less than 20 percent of the causes of severe accidents involving these marine structures can be attributed to the environment. The rest were due to initiating events such as groundings, fire, explosions, and collisions. In almost all cases, the initiating event can be traced to a catastrophic compounding of human and organizational errors (Heising and Grenzebach, 1989; Offshore Certification Bureau, 1988; Panel on Human Error in Merchant Marine Safety, 1976; Report of the Royal Commission on the *Ocean Ranger* Marine Disaster, 1985).

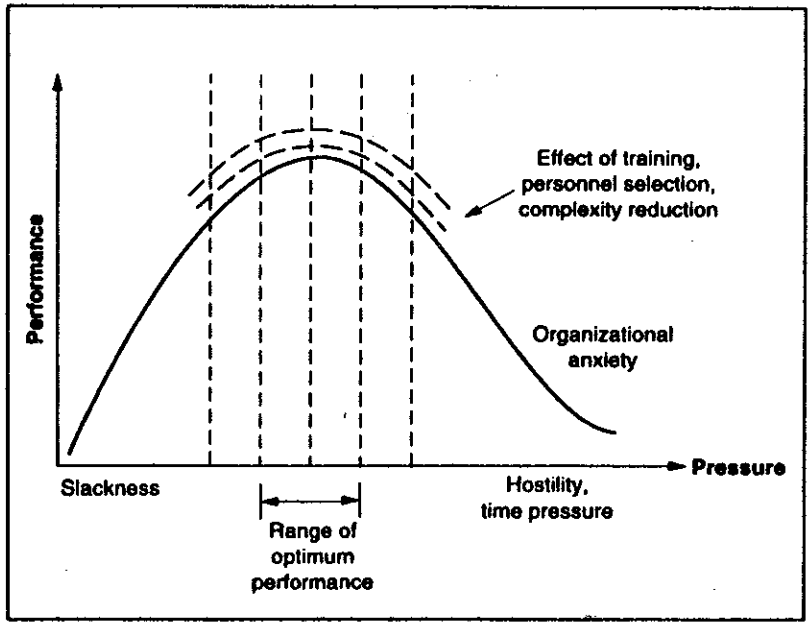
Table 11-1 shows a taxonomy of a number of factors that can result in human errors. The errors range from those of judgment to "ignorance, folly, and mischief" (Panel on Human Error in Merchant Marine Safety, 1976; Wenk, 1986). These errors are magnified and compounded in times of stress and panic (Heising and Grenzebach, 1989; Offshore Certification Bureau, 1988; Panel on Human Error in Merchant Marine Safety, 1976; Wenk, 1986). As shown in Figure 11-3, optimal performance levels are observed at an "appropriate level

Table 11-1
Human Error Factors

Fatigue	Wishful thinking	Bad judgment
Negligence	Mischief	Carelessness
Ignorance	Laziness	Physical limitations
Greed	Drugs	Boredom
Folly	Mischief	Inadequate training

of arousal" (Melchers, 1976). Human performance levels vary between individuals depending upon training, variability among individuals, organizational pressures, and complexity of the operating system. Performance deteriorates when pressure levels are either too low or too high. For example, stress or panic can produce high pressure while boredom or laziness produces low pressure. Both extremes can contribute to increased incidence of human errors. Foushee and Lauber (this volume) provide evidence of yet other forces that contribute to poor performance.

Figure 11-3
Human Performance Function



Source: Melchers, 1987

Modeling a Simple Mishap

Studies of the role of human errors in the reliability of engineered structures indicate that human errors and imperfections basically are inevitable (Bea, 1989; Ingles, 1985; Nowak, 1986). Figure 11-4 provides a schematic description of a simple mishap. Once a mishap is initiated, the objective is to return the system to normal before it reaches a critical threshold.

A mishap is differentiated into three psychological factors: *perceiving*, *thinking*, and *acting*. The danger threshold could be reached by lack of sufficient time to react, or errors in perception, thought, or action that would either lengthen the time between events or increase the magnitude of the danger buildup. The perception stage starts with a mishap and is followed by a warning signal (see Figure 11-5). The warning is then noticed and leads to recognition of the mishap source. The thinking stage begins with identification of the problem, and information (whether complete or incomplete) is processed at this stage to evaluate decisions for the best course of action. The mishap is acted upon with execution of a plan, and the system is returned to a normal operating status or escalates to a dangerous state.

Figure 11-4
A Simple Model of a Mishap

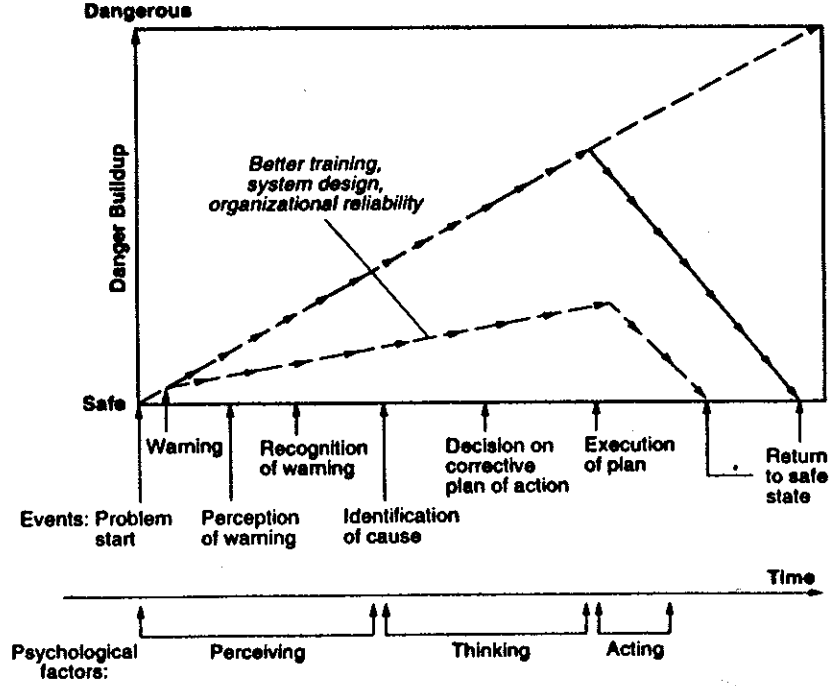
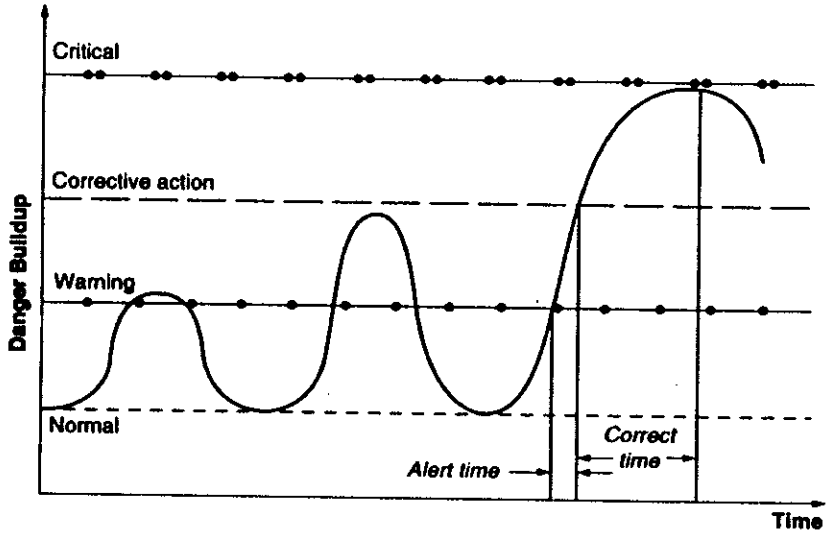


Figure 11-5
Danger Buildup Function



Source: Paté-Cornell, 1986

Though errors occur, they are influenced by cultural and moral values, corporate responsibilities and organizations, and individual training, craftsmanship, and integrity. The individual, organizations, and societies all play important roles in human errors that lead to dangerous states and that can result in catastrophic consequences.

ORGANIZATIONAL ERRORS

Analyses of past decisions regarding operating offshore platforms provide numerous examples of instances in which organizational deficiencies resulted in marine system failures (Heising and Grenzebach, 1989; Moan, 1983; Panel on Human Error in Merchant Marine Safety, 1976; Paté-Cornell and Bea, 1989; Report of the Royal Commission on the *Ocean Ranger* Marine Disaster, 1985; Veritec, 1988). Both collections of individuals (organizations, societies) and individuals (unilateral actions) contribute to accident situations. Failures can occur because of an organization's or an individual's willingness to take calculated risks (Arrow, 1951; Arrow, 1972). Failures can result from different types of inevitable errors that can be corrected in time, provided they are detected and recognized as errors, and corrective action is promptly taken (see Figures 11-4 and 11-5). Failures can also occur as the result of errors or bad decisions, most of which can be traced back to organizational malfunctions.

Table 11-2 shows a number of factors that can have negative effects on organizational reliability. For example, the goals set by the organization may lead rational individuals to conduct operations aboard a platform in a manner that corporate management would not approve if it were aware of their reliability implications (Howard, 1966; Kahneman, Slovic, and Tversky, 1982; Roberts, 1990). Similarly, corporate management, under pressure to reduce costs and maintain schedules, unknowingly may not provide the necessary resources required to promote safe operations. Hirschhorn (this volume) lays blame squarely on management's shoulders, as well as on required procedures for deteriorating performance in a nuclear power plant.

Generally, two classes of problems face an organization in making collective decisions that result from sequences of individual decisions: ***information*** (who knows what and when?), and ***incentive*** (how are individuals rewarded, what decision criteria do they use, how do these criteria fit the overall objectives of the organization?) (Arrow, 1972; La Porte, 1988). In developing programs to improve management of HOE, careful consideration must be given to information (collection, communications, and learning) and incentives, particularly as they affect the balancing of several objectives such as costs and safety under uncertainty in operations of offshore platforms (Foushee and Lauber, this volume; Weick, 1987; Wenk, 1986).

The structure, the procedures, and the culture of an organization contribute to the safety of its product (Kahneman, Slovic, and Tversky, 1982; La Porte, 1988; Schulman, this volume) and to the economic efficiency of its risk management practices (Royal Norwegian Council for Scientific & Industrial Research, 1979; Wenk, 1986). The organization's structure can be unnecessarily complex and may demand flawless performance. This can result in little or no credible feedback to upper levels of management (see Hirschhorn, this volume). The resulting safety problem may ensue because there are inconsistencies in decision criteria (e.g., safety standards) used by the different groups for various activities. This can result in large uncertainties about the overall system safety, about the reliability of the interfaces, and about the relative contribution of different subsystems to overall failure probability (Construction Industry Research and Information Association, 1977; Moan, 1983; National Bureau of Standards, 1985).

Organization and management procedures that affect system reliability include, for example, parallel processing such as developing design criteria at the same time as the structure is being designed, a procedure that may or may

Table 11-2
Organizational Error Factors

Time pressures	Culture	Incentives
Cost–profit incentives	Morale	Communications
Regulatory requirements	Promotion—recognition	Production orientation

not be appropriate in economic terms according to the costs and the uncertainties (Bea, 1989; Paté-Cornell and Bea, 1989).

The culture of the organization can also affect system reliability (Arrow, 1972; Roberts, Rousseau, and La Porte, in press; Weick, 1987; Wenk, 1986). For example, the dominant culture may reward risk-seeking (flirting with disaster) or superhuman endurance (leading to excessive fatigue), an attitude that in the long run may prove incompatible with the objectives of the organization. Another feature may be the lack of recognition of uncertainties leading to systematic biases towards optimism and wishful thinking (Panel on Human Error in Merchant Marine Safety, 1976; Paté-Cornell and Seawell, 1988).

SYSTEM ERRORS

Errors can also be exacerbated by poorly engineered systems that invite them. Such systems are difficult to construct, operate, and maintain (Ingles, 1985; Melchers, 1987; Moan, 1983). Table 11-3 shows a taxonomy of system flaws that can affect marine systems. New technologies compound the problems of latent system flaws. Complex design, close coupling (failure of one component leads to failure of other components) and severe performance demands on systems increase the difficulty in controlling the impact of human errors even in well-operated systems (Perrow, 1984). Emergency displays have been found to give improper signals of the state of the systems (Heising and Grenzebach, 1989; Lord Cullen Report, 1990; Perrow, 1984; Report of the Royal Commission on the *Ocean Ranger* Marine Disaster, 1985). Land-based industries often can spatially isolate independent subsystems whose joint failure modes would constitute a total system failure. System errors resulting from complex designs and close coupling are more apparent due to spatial constraints aboard ships and platforms. For example, spatially isolating the accommodations unit on *Piper Alpha* could have substantially reduced the loss of life aboard the platform: 82 men died in the accommodations unit (Lord Cullen Report, 1990).

Human performance is a function of the lead time available to respond to warnings in the system. Errors are compounded by the lack of effective early warning systems (Paté-Cornell, 1986). As observed in Figure 11-5, if the lead time is short, there is little time allowance for corrective action before the situation reaches a critical state. On the other hand, if the system is too sensitive, resulting in frequent false alarms, operators will eventually cease to respond to warning signals. The time differential between the normal and

Table 11-3
System Error Factors

Complexity	Latent flaws	Severe demands
Close coupling—non-redundancy	Small tolerances	False alarms

warning stages are dependent upon the sensitivity of the system to developing danger. However, as shown in the mishap model (see Figure 11-4), adequate human performance is critical at the initiation of an alert stage (warning) and in expedient execution of a plan (corrective action) to bring the system back under control.

ALTERNATIVES TO IMPROVE MANAGEMENT OF HOE

In many cases, a combination of human, organization, and technical (system) modifications can improve overall safety. Table 11-4 lists some effective human, organizational, and technical factors that can benefit operational reliability.

After a catastrophic failure, technical modifications are frequently proposed to "fix the problem." An example is the legislation requiring double-hull tankers following the *Exxon Valdez* disaster. (One wonders if this legislation took into account the reduction of cargo capacity of double-hull tankers. This will result in more tanker traffic to maintain capacities and increase the risk of other types of accidents such as collisions.) Technical modifications, however, represent only one class of risk management strategy. When a system's failure is studied after the failure occurs, it is often obvious that what resulted in a technical failure was actually rooted in a functional failure of the organization and the human operators (Arrow, 1972; March and Simon, 1958). Organizational modifications may address some of the reliability questions at a more basic level than at strengthening the engineering design alone. These include, for example, improving communications, setting effective warning systems, and ensuring consistency of standards across the organization. Rochlin and Schulman (this volume) focus specifically on organizational mechanisms to ensure safety in high reliability organizations. Creed, Stout, and Roberts (this volume) narrow in on the effectiveness aspect of these mechanisms.

There is a current misconception that new technologies are necessarily better than old ones. But new technologies create new sets of problems and additional risks (Wenk, 1986). As technological systems become more efficient and attractive (also more complex), we have a tendency to forget that these systems pose exceptional risks. The following examples demonstrate the need

Table 11-4
Error Management

Human	*Organization*	*Systems*
Selection	Resource allocation	Human tolerances
Training	Communication systems	Redundancy
Licensing	Decision making	Early warning systems
Verification	Process orientation	Damage tolerances
Incentives	Integrity	
Job design	Accountability	

for a combination of human, organizational, and system management to ensure operational reliability.

CASE HISTORIES

Development of accurate case histories of past marine accidents can provide a basis for defining how the interactions of systems, humans, and organizations can lead to such disasters. These interactions provide templates with which new and existing systems can be studied to determine how best to prevent catastrophic compounding of HOE ("Those who don't know history are destined to repeat it"). To illustrate the process, three case histories of marine accidents are developed.

Ship Pump Room Gas Detector

A shipping company operated its vessels with twenty-five crew members since 1955. In 1982, the first engineer and a pumpman were seriously injured in an accident in the pump room when a gas leak ignited. The company managers decided to place in a pump room gas detection and an emergency shutdown system that could be operated from the bridge. In addition, to cut costs and the chances of injury to crew members, the vessels were operated with a single day-shift engineer (instead of three or four engineers) and no pumpman since the pumping system was totally automated and operational from the bridge. The company also believed the new technology was attractive since pump and engine room maintenance crews could be brought aboard at ports of call and need not accompany the ships during transit, thus reducing operating costs (as well as ship maintenance).

No major problems developed with gas leaks aboard the vessel until 1991 when a leak again occurred in the pump room. The bridge operators, having not had any problems with this system over nine years, paid little attention to the gas detection gauge on the bridge console (early warning signal), and did not shut down the system before an explosion and fire occurred. In addition, over the last eight years, the company employed a day engineer whose specialties were not mechanical systems, but electrical systems to keep pace with the new automated technologies implemented over the years.

The day engineer, having little experience with these types of problems, could not control the fire automatically, nor was there manpower to fight the fire effectively since the size of the crew had been reduced. The ensuing fire escalated and reached the engine room. The result was a power plant failure while the ship transited an area with many navigational hazards. The ship sent a "mayday" for assistance since it was drifting towards a hazardous reef. Assistance did not arrive in time and the ship ran aground, spilling 200,000 barrels of oil in an environmentally sensitive area.

The point of this example is that new technological systems carry their own set of risks. This scenario demonstrates human errors (improper bridge monitoring, inadequate training), organizational errors (ship managers cutting back on manpower), and system errors (inadequate systems to prevent, detect, control and fight the fire). In addition, it exemplifies the overconfident trust placed on a technological system (gas detection, emergency shutdown systems, and automatic control from the bridge) without attention to the potential risks associated with it. The monitoring system had been changed from an active system (engineers and pumpmen working around the clock) to a passive system (gas detection and bridge control). Technological "fixes" did not control the problem but only created new failure scenarios.

Mobile Drilling Unit Ballast Control System

A floating mobile offshore drilling unit (MODU), operating off the east coast of Newfoundland, encountered a severe North Atlantic storm. As the intensity of the storm increased, the drilling unit suspended operations. Late in the evening, a large wave broke a port light in the ballast control room; the port light cover had not been put in place. Water entered the ballast control room, resulting in an electrical failure of the ballast control console. This made it difficult to assess the amount of ballast in the ballast tanks and to determine if the valves between tanks were open or closed. Manual ballast control could be conducted from the pump rooms at the stern of the pontoons that provided buoyancy to support this unit.

Valves between the ocean and ballast tanks could be operated manually from the control room in the event of an electrical failure. However, the ballast control personnel were under the assumption that the insertion of solenoid rods into the ballast control console closed the valves between tanks, when actually the rods opened them. As water entered the forward ballast tanks, the MODU began to list forward. By early morning, heavy seas began to break on the upper deck of the platform, resulting in water entering the mooring chain lockers; the unit slowly turned itself over and began to sink.

An SOS resulted in emergency rescue aircraft being dispatched to the scene. However, due to the severe weather, the emergency rescue aircraft could do little to help and had to return to land. Crewmen donned life jackets, but there were no exposure suits for protection against the cold 31-degree water. Personnel were clad in both light and heavy clothing; the order to abandon the MODU came at the last minute.

A standby support vessel in the vicinity of the MODU attempted to save the crew, but because of the vessel's inadequate design for rescues and the lack of formal rescue training of the ship crew, the attempt proved futile. Due to the extreme list of the MODU, only one lifeboat could be successfully launched. That lifeboat capsized alongside the rescue boat when water entered an open hatch and everyone moved to one side of the lifeboat to evacuate. In the water, the crewmen were quickly immobilized and died due to hypothermia. Nine hours after the port light had been broken, the MODU sank to the bottom of the North Atlantic. All eighty-four crewmen perished.

Not a single person aboard the MODU had a clear understanding of how to operate the ballast control system correctly. The organizational structure onboard the MODU was complex. The *tool pusher* is responsible for decisions regarding the safety of the rig, yet he had no experience with ballast control on floating drilling units. The *drilling foreman* is in charge when the rig is drilling and is the only person who has the authority to activate the standby support vessel and rescue aircraft. The *master* is responsible for supervising and training ballast control operators, loading and unloading operations, and general maintenance of the MODU. The particular master assigned to this MODU was a former mariner on temporary assignment who had no experience in ballast control. His *senior and junior ballast control operators* had no formal training in ballast control and were not familiar with the ballast control system onboard this particular MODU. Ten days prior to the accident, the master had made an error in the ballast control that resulted in a significant list of the rig. The shore-based operations management was aware of the situation; however, they chose not to replace the master since he was on temporary assignment. The senior and junior ballast control operators were placed onboard in response to regulations regarding the employment of local personnel.

This example illustrates the interrelationships of a complex and poorly designed system (ballast, evacuation), inadequate training, poor organization and supervision, and the lack of an effective rescue and safety contingency plan. Influences of the individual operators, the organization, and the society are clearly evident.

Platform Maintenance Operations

The night shift had just taken over operations onboard a fixed platform in the North Sea. The control room personnel were waking up and a contract maintenance crew had started working on one of the gas condensate pumps that was not working properly (there were two of these pumps). These pumps inject liquids or condensate from the produced gas into the oil production system.

The production superintendent was assisting the maintenance crew in determining the source of the problem. Gas being produced from the platform and from two adjacent platforms and sent via pipeline to the platform placed the platform on a code red status, indicating a maximum production situation. The production superintendent normally onboard the platform was on vacation. His position was filled by a replacement superintendent who had just come onboard the platform.

Earlier in the day, maintenance work was partially completed on the other condensate pump; it had been taken out of service to maintain its safety equipment, but the work had not been completed before the night shift took over. The control room personnel were unaware of the maintenance work. Also, earlier in the day, divers had been in the water working on the underwater portions of the platform, and the fire pumps and deluge system (similar

to a sprinkler system in a building) had been placed on manual control to prevent divers from being sucked into the seawater intakes.

The malfunctioning condensate pump (which injects liquids from the gas stream into the oil pipeline) failed, and the order was given to the control room to turn on the other pump to avoid condensate from backing up into the gas compressors. The control room personnel did not realize that the other pump was not working and opened the valves to the pump, routing the gas condensate to the inoperable pump. Condensate and gas escaped into the module and ignited with a deafening explosion, killing the crew and production superintendent. Due to the containment of the explosion, the adjacent control room was decimated. Power was lost due to destruction of the primary electrical wiring system by the explosion. The automatic deluge and emergency power systems did not come on because they had been placed on manual control and could not activate the systems manually as a result of the fire.

The fire quickly spread to adjacent oil- and gas-producing vessels and piping. Unprotected fuel storage above the gas compression module was ignited, and thick, dense, toxic smoke engulfed the quarters where surviving crew members were being mustered for evacuation in life boats. While the crew was awaiting the orders from the production superintendent to evacuate, fresh air intake fans sucked the smoke into the quarters. Because the production superintendent was killed in the initial explosion, the evacuation orders never came, and in the dark and confusion the crew members were overcome by smoke and died.

Moored adjacent to the platform was an emergency support vessel. This vessel was designed specifically to provide emergency support to fight fires, kill well blowouts, accommodate divers and other field personnel, and provide emergency medical facilities. The vessel was instructed to fight fires at the order of the production superintendent. Again waiting for orders that could never come, and fearing for the safety of the vessel, the vessel master gave orders to pull back from the escalating fire. The fire fighting pumps were never used.

Pipelines bringing oil and gas from the adjacent platforms passed immediately under the platform. Subjected to intense heat, these lines softened and ruptured. A deafening explosion and fireball engulfed the entire platform. The emergency shut-in devices (to prevent the pipeline contents from escaping) were in the same area and were destroyed, allowing the pipeline contents to be emptied into the fire.

The result of these developments was total destruction of the platform and loss of 167 lives. The accident was the result of design flaws, human, organization, and societal factors. The platform owner was aware of the marginal situation onboard the platform before the incident; wishful thinking and shortsightedness (emphasis on present profitability) were evident. The regulatory body responsible for overseeing the operations was similarly aware of the situation but was unable or reluctant to force compliance with already lax safety

guidelines. The operating personnel had operated the platform at its code red or maximum operating level only once before in the rig's lifetime; this occasion had occurred at a time when the experience level was marginal. The capacity of the equipment systems was stretched to the breaking point. What appeared to be redundant critical systems (the two condensate pumps, deluge system) were not really redundant. They could not be safety operated. Similarly, the onboard organization contained critical flaws that did not provide adequate backup or redundancy. Given the death of the production superintendent, the organization became dysfunctional in an emergency situation. Poor communications and work procedures (the day crew did not brief the night crew) exacerbated and eventually triggered the disaster.

PROBABILISTIC RISK ANALYSIS (PRA)

If HOE affects a subsystem whose functioning is not highly critical, its effect on overall system reliability may be minor and may not justify profound human or system changes. However, complex interactions of relatively independent subsystems can substantially affect overall system reliability due to system complexities and tight coupling (Perrow, 1984). If deficiencies affect a subsystem or a complex interaction of subsystems whose failure constitutes a system failure mode, it is urgent to address the problem at its human and system origins, as shown in the previous example. To permit evaluations of the interactions of the human and system components, it is desirable to organize and assess these features in a *probabilistic risk analysis* (PRA) (Moan, 1983). This allows one to develop insights into the urgency of remedial measures, to evaluate alternative remedial measures to improve safety, and to set priorities among HOE problems to be addressed.

A PRA for engineering systems allows identification of the weakest parts of a system through qualification of the probabilities of the different failure modes (Melchers, 1987). Event tree modeling, a form of PRA, has been found to be an effective method to analyze contributions of individual accidents to risk associated with offshore operations (Larocque and Mudan, 1982). This technique permits setting priorities among possible modifications aimed at the reduction of the failure risks and, therefore, optimal allocation of limited risk management resources.

The general method is to integrate elements of process analysis and organizational analysis in the assessment of the probability of system failure (Bea, 1989; Paté-Cornell and Bea, 1989; Paté-Cornell and Seawell, 1988). Figure 11-6 provides a schematic description of the structure of this integration model. The first phase (which does not appear in this diagram) is a preliminary PRA to identify the key subsystems or elements of the system's reliability. The second phase is an analysis of the process to identify the potential problems for each subsystem and their probabilities or base rates per time unit or per operation.

The next phase is to analyze organizational procedures and the incentive system to determine their influence on the occurrence of basic errors and the

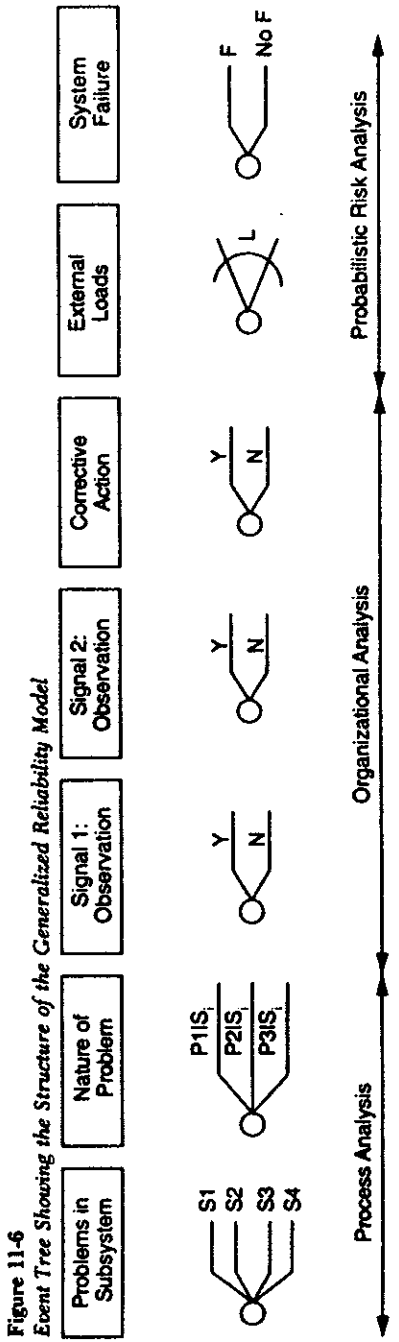


Figure 11-6
Event Tree Showing the Structure of the Generalized Reliability Model

Source: Paté-Cornell and Bea, 1989

probability that they are observed, recognized, communicated, and corrected in time (i.e., before they cause a system failure).

The result of these three phases is a computation of the probabilities of the different system states corresponding to possible types of structural defects and, therefore, to different levels of systems capacity. The fourth phase involves a return to the PRA for the physical system and a computation of the probability of failure for each capacity level corresponding to the different system states.

The overall failure probability is then obtained. It explicitly includes the possibility of weaknesses in the different subsystems due to organizational structure. These different models (process, organization, and final PRA) are integrated using an event tree (Heising and Grenzebach, 1989; Nessim and Jordan, 1985) or influence diagram (Shachter, 1986) to compute the failure probability under different circumstances (such as occurrence and correction of a given problem in the process). We propose here to quantify the benefits of organizational measures, using PRA as a starting point.

One can quantify the costs and benefits of HOE reliability management measures using PRA (Heising and Grenzebach, 1989; Moan, 1983; Nessim and Jordan, 1985). The analysis of a system's reliability allows identification of its failure modes and computation of their probabilities. It permits a decision maker to choose technical solutions that maximize an objective function (costs and reliability) under resource constraints (Weick, 1987; Wenk, 1986). These solutions include, for instance, the choice of operating procedures and equipment that minimize the probability of failure during the lifetime of a structure under constraints of safety budgets, costs, time to completion, production level, structure location, and general type. The results of the analysis can provide valuable insights into where scarce safety resources can best be deployed to achieve the largest improvements in safety.

Operations Example: Event Tree Analysis

An example helps illustrate the basic tenets of a marine HOE PRA. The example is the installation of an emergency shut down (ESD) valve in an existing pipeline.[2] Three HOE management alternatives will be considered:

Alternative 1. Use the present system.

Alternative 2. Allow for modest improvements in the planning, training, and supervision involved in the operation.

Alternative 3. Allow for major improvements in planning, training, and supervision.

[2]A major fire recently destroyed a Gulf of Mexico platform during installation of an ESD into an existing pipeline (Minerals Management Service OCS Report, 1990).

Based on data developed on the performance reliability of each of these three alternatives, Table 11-5 summarizes the probabilities of a successful operation in each stage of installing the ESD.

The probabilities of successful operations of Alternatives 2 and 3 were based on one and two levels, respectively, of checking the normal operation characterized as Alternative 1. The probability of successful detection and correction of error signals developed in each phase of the operation in Alternative 1 (no checking) was assigned a probability of 0.5 and in Alternative 2 (one level of checking). The same probability of detection and correction was assigned in Alternative 3 (two levels of checking).

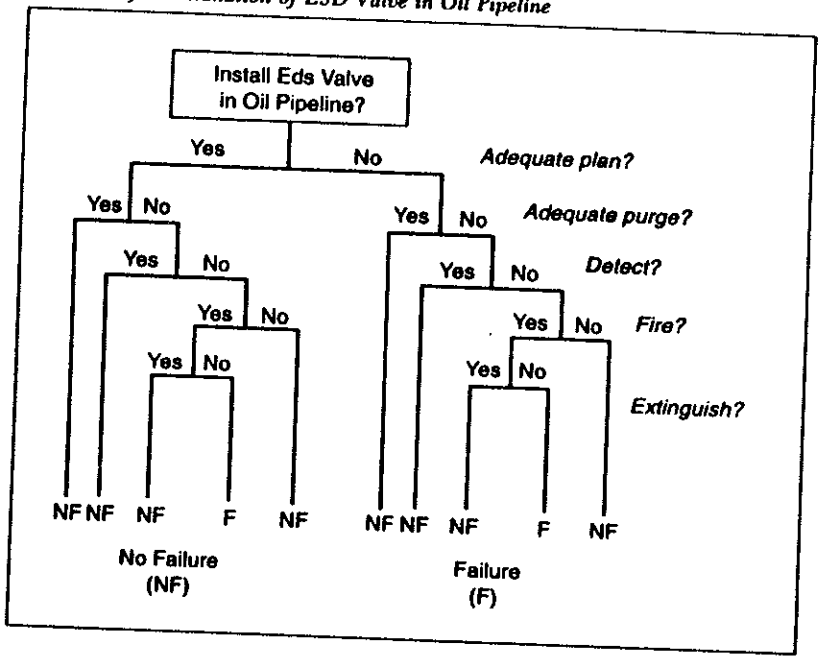
In an actual PRA, these probabilities are based on results from studies of operations comparable to those of Alternative 1 and of the likelihoods of checking and corrective action given specified procedures for such actions. At the present time, such data are generally lacking for HOE PRA, and this poses one of the major hurdles to the performance of realistic quantitative analyses. Some organizations have begun to develop such information (Veritec, 1988) and more will be developed in the course of the research summarized previously in this chapter.

Figure 11-7 shows an event tree for installing an ESD valve in an oil pipeline. The event tree distinguishes between decisions and events at various states of the system. Table 11-6 summarizes the results of the HOE PRA, indicating the probabilities that fires caused by the ESD installation operation are not extinguished before there is significant damage to the platform. In addition, the estimated costs associated with the installation of the ESD using each operation alternative is shown together with the expected total estimated costs associated with fires. The costs associated with the fires have been estimated at between one and two million dollars.

Table 11-5
Probabilities of Successful Operations

Phase of Operation	*Alternative 1*	*Alternative 2*	*Alternative 3*
Adequate planning of ESD installation	0.50	0.75	0.875
Adequate purging of pipeline	0.50	0.75	0.875
Detection of hazardous hydrocarbons	0.50	0.75	0.875
Suppression of explosion and fire	0.50	0.25	0.125
Extinguishment of fire before significant damage	0.50	0.75	0.875

Figure 11-7
Event Tree for Installation of ESD Valve in Oil Pipeline

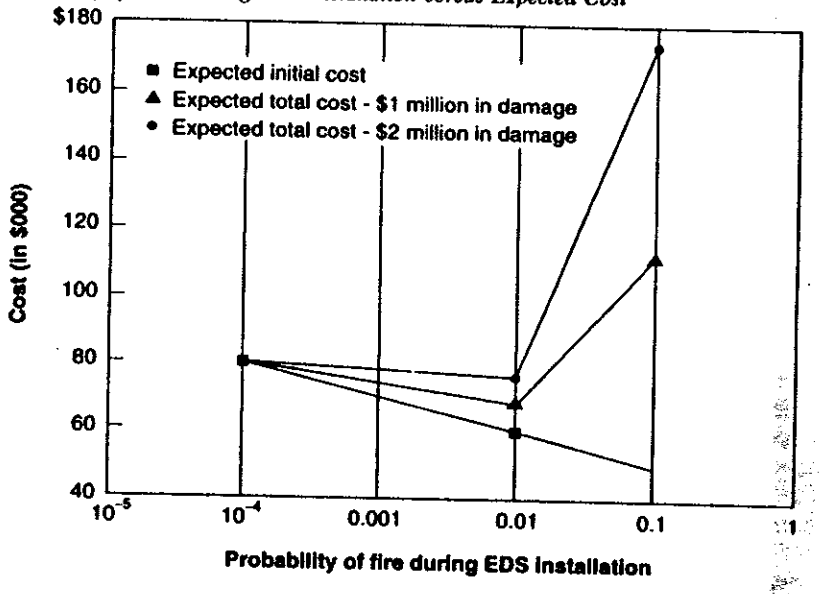


As shown in Figure 11-8, the increase in initial cost to make radical improvements to the operations to reduce the probability of fire during ESD installation ($30,000) does not appear to be economically justified. The $10,000 investment to make moderate improvements appears to be well-justified by the

Table 11-6
Probabilities for Expected Costs for Operational Alternatives

Operation Alternative	Probability of Fire During Operations	Estimated Initial Cost ($000s)	Expected Total Cost: $1 million damage cost ($000s)	Expected Total Cost $2 million damage cost ($000s)
Present system	0.0625	$50.0	$112.5	$175
Moderate improvements	0.0081	60.0	68.1	76.2
Major improvements	0.0001	80.0	80.1	80.2

Figure 11-8
Probability of Fire During ESD Installation versus Expected Cost



range of reduction in expected total costs. Additional study could be performed to determine which of the changes in the operations phases are most effective at reducing the likelihoods of fires.

As a footnote to this example, after the platform disaster described in the previous section occurred, the industry quickly reacted and some operators began installing emergency shut-in valves on gas and oil import and export pipelines. One of these operations required cutting an existing pipeline prior to inserting an emergency shut-in valve. The pipeline had been purged of gas and oil prior to the start of the work. The inexperienced work crew (selected on the basis of low bid) ignored the warning work crew (selected on the basis of low bid) ignored the warning signs when oil and gas began to leak from the pipeline they were cutting. A fire started and was quickly followed by a massive explosion. The platform was engulfed by flames fed from the pipeline that had not been completely purged. The result was again total destruction of the platform and the loss of seven lives.

Influence Diagramming

Influence diagramming is a form of PRA modeling that allows flexibility in examining HOE and HOE management alternatives. There are distinct advantages for using influence diagramming for PRA. In standard decision tree analysis, decisions are based on all preceding aleatory and decision variables.

However, not all information is available to a decision maker, and information may come from indirect sources or not in the specific order in which the decision tree is modeled. When using influence diagramming, all nodes need not be totally ordered. This allows for decision makers who agree on common based states of information, but differ in ability to observe certain variables in the diagramming.

Modeling of Pump Room Fire Scenario: Manual vs. Automated System

Let us now return to the pump room example described previously. Using the influence diagram shown in Figure 11-9, we can consider two alternatives for emergency gas detection and shutdown in a tanker pump room: Alternative 1—manual monitoring of the pump room by an engineer and pumpman on duty around the clock, and Alternative 2—installing an emergency gas detection and shutdown system that is operated from the bridge. These alternatives are examined to determine the eventual failure probabilities of the power plant resulting from fires initiated by pump room gas leaks. Each single-border oval or circular node shown in Figure 11-9 describes probabilistic nodes while double-border nodes describe deterministic values in the model. Table 11-7 shows the probabilities of a gas leak in the pump room.

Figure 11-9
Influence Diagram of Effects of Gas Leak in Tanker Pump Room

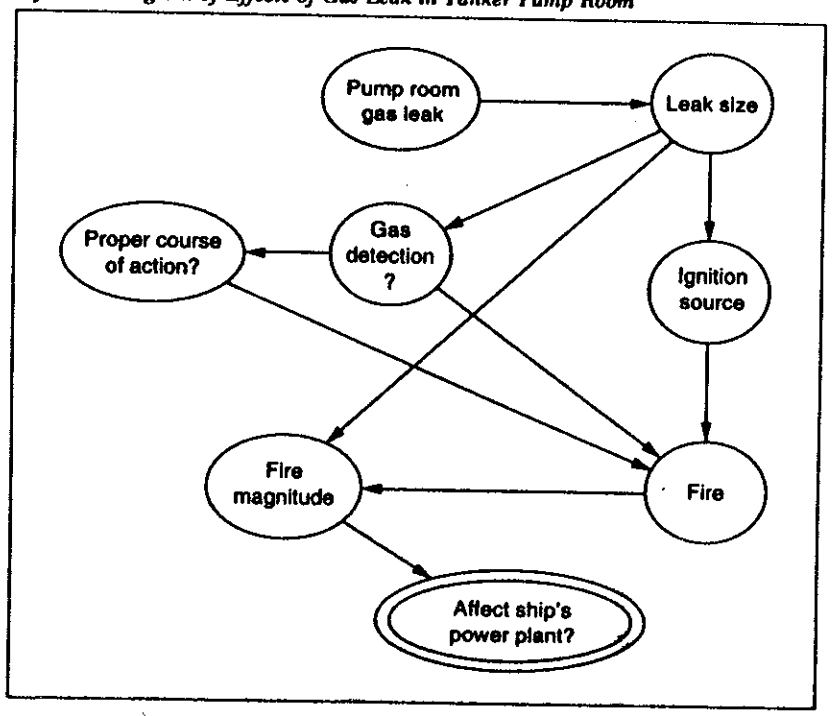


Table 11-7
Probability of a Pump Room Gas Leak

Gas leak (GL)	.005
No gas leak (NGL)	.995

Table 11-8
Probabilities of Pump Room Gas Leak Sizes

Small leak (SL)	.70
Moderate leak (ML)	.25
Large leak (LL)	.05

Table 11-9
Probability Distribution of a Pump Room Gas Leak Detection Before Ignition

Pump Room Gas Leak	*Leak Size*	*Gas Detection*	*Probability of Detection (GDS)*	*Probability of Detection (operators)*
Leak	Small	Yes	.90	0.75
		No	.100	0.25
	Medium	Yes	.990	0.85
		No	.010	0.15
	Large	Yes	.999	0.95
		No	.001	0.05
No leak	No leak	Yes	0.00	0.00
		No	1.00	1.00

A probability distribution is established for the magnitude of the leak and is represented by the "leak size" node. Table 11-8 shows this probability distribution for leak sizes. The leak size influences three factors: (1) the detection of gas, (2) the ignition of the leak, and (3) the magnitude of the fire. Gas detection is assumed to be dependent upon its concentration in the ambient atmosphere around either the pump room operators (detection by smell, sound, or gauging) (see Table 11-8) or the automatic gas detection system (GDS) (Table 11-9). Gas detection is a step process for both manual and automatic operations: it involves a warning signal followed by the problem recognition, identification, and execution of a plan (see Figure 11-4). The larger the leak, the greater the chance of detection. Table 11-9 displays the conditional probability distribution for gas detection dependent upon the initiation of the leak and its size. In addition, the gas must locate an ignition source for a fire to be

Table 11-10
Probabilities of Gas Leaks Finding Ignition Sources

Leak Size	Ignition Source	Probability of Ignition Source Being Located
Small	Found	.40
	Not found	.60
Medium	Found	.70
	Not found	.30
Large	Found	.95
	Not found	.05
No leak	Found	0.00
	Not found	1.00

Table 11-11
Probabilities of Controlling Gas Leak

Gas Detection	Leak Controlled	Probability Using Manual Operation	Probability Using GDS System
Yes	Yes	.90	.60
Yes	No	.10	.40
No	No	1.00	1.00

initiated. The model assumes that the greater the magnitude of the gas leak, the greater the probability it finds an ignition source, as shown in Table 11-10.

The "proper course of action?" node in Figure 11-9 models whether operators were able to return the system to a normal state by intervening to prevent the fire from occurring. The distributions shown in Table 11-11 demonstrate two factors: (1) the probability of manual control of a leak or fire is greater than that of automatic control since both manpower and mechanical expertise are available to extirpate the problem, and (2) passive monitoring from the ship's bridge can lead to a limited alert time before escalation to a state that is impossible to control (see Figure 11-5).

As shown in Figure 11-9 fire initiation, presented by the deterministic node "fire," depends on three factors: (1) whether the gas was detected, (2) whether a proper course of action was carried out to control the leak if detected, and (3) whether the gas located an ignition source. Table 11-12 shows the conditions in which a fire occurs.

As represented in Figure 11-9, "fire magnitude" is dependent upon both the size of the leak and fire occurrence. The larger the gas leak, the greater the chance of a large-magnitude fire. These assumptions are represented by the probabilistic distributions shown in Table 11-13.

Finally, due to the proximity of the pump room to the main engine room, the magnitude of the fire will have an effect on the probability of failure of the ship's power plant. The fire events represented by the fire magnitudes will

Table 11-12
Conditions to Initiate Fire Event

Ignition Source Located	Leak Controlled	Gas Detected	Fire Event
Yes	Yes	Yes	No fire
Yes	No	Yes	Fire
Yes	No	No	Fire
No	Yes	Yes	No fire
No	No	Yes	No fire
No	No	No	No fire

Table 11-13
Probability Distributions of Fire Magnitudes

Leak Size	Fire Event	Fire Magnitude	Probability of Fire Magnitude
No leak	Fire	No fire	1.0
	No fire	No fire	1.0
Small	Fire	Small	.75
	Fire	Moderate	.175
	Fire	Large	.075
	No fire	No fire	1.0
Medium	Fire	Small	.25
	Fire	Moderate	.5
	Fire	Large	.25
	No fire	No fire	1.0
Large	Fire	Small	.2
	Fire	Moderate	.4
	Fire	Large	.4
	No fire	No fire	1.0

Table 11-14
Probabilities of Plant Failures for Operational Alternatives

	Probabilities of failure
Manual operated system	
Fire	7.58×10^{-4}
Plant failure	3.11×10^{-4}
Automatic GDS	
Fire	1.33×10^{-3}
Plant failure	6.19×10^{-4}

determine whether the power plant is operational. It is assumed that if the fires are small, they can be effectively controlled and so pose no threat to the integrity of the power plant. If the fire is moderate or large, however, the integrity of the power plant is affected and the plant fails (this may be due to heat or flame moving from the pump room to the engine room).

Based on the assumptions of the probabilistic and deterministic variables discussed above, Table 11-14 summarizes both the failure probabilities of the power plants and the conditional failures of the power plants dependent upon fire events. Though the automatic GDS is better at detecting gas leaks than are human operators, the probabilities of fires for the manual system are approximately half those of the GDS system. This is primarily the result of the limited ability to control a fire due to limited manpower. Similarly, the probabilities of plant failures for the automated system are approximately twice that of the manual system. These results should lead decision makers to reevaluate the implementation of the automatic system. This scenario exemplifies the need for closer analysis of new technology systems.

CONCLUSIONS

In traditional reliability-based studies of ships and offshore platforms, HOE is implicitly integrated into the background of accident statistics and experience on which such studies are often based. The principal focus of these studies has been the structural aspects or the equipment aspects and how design may be modified to improve reliability.

Recently we have come to recognize that we may have been working on only a small part of the problem of marine system reliability. Given that some 80 percent of major accidents can be traced directly to HOE, it seems appropriate for engineers to evaluate explicitly how marine systems and the humans that are an integral part of them from their design to their decommissioning can be better configured to improve safety.

Our research and experience indicate that the majority of high-consequence, low-probability marine accidents have one common theme: *a chain of important errors made by people in critical situations involving complex technological and organizational systems. Many of these errors involve fatigue, carelessness, negligence, short sightedness, greed, lack of training, and wishful thinking.*

The errors go beyond individuals directly involved in the incidents. In some cases, organizations provide "cultures" that invite excessive risk taking, demand superhuman performance, and develop complacency that results in reactive risk management. Shortsightedness, with a central focus on present profitability, seems to be a primary factor in such cultures. Industry, government, and society all share in providing them. This is a far cry from organizational descriptions presented by Schulman and Rochlin (this volume), but it is close to the picture painted by Hirschhorn (this volume).

In some cases, we engineer marine systems that cannot be constructed and operated as they should, so field modifications and short cuts must be developed. The engineer rarely hears about these problems until they become critically evident. People are transferred so rapidly and in some cases retired so early that there is a loss of corporate memory of these mistakes. Unnecessary complexity in systems (physical and organizational) invites errors. When we engineer overly

complex systems, and place them in the hands of improperly trained, unmotivated people, we ask for the trouble we have been experiencing.

The human and organizational elements of marine systems must be engineered and designed, just as we engineer the physical elements of these systems, and each of these needs to complement the other. We must learn how to engineer systems to be more forgiving and tolerant of errors and flaws: people tolerant systems. We must honestly recognize the potential blindness produced by our pride, our enduring trait of wishful thinking, our limitations (fatigue, boredom, confusion, ignorance), our reckless ways (drug abuse, greed, lack of integrity), and the differences between what we know we should do and what we actually will do.

The HOE problem must be attacked at the level of the individual: through training, testing, motivating, and by verifying to a degree commensurate with the job to be performed and the needs for safety in the job. People must be trained in managing crisis situations in the systems they operate. Reducing complexity of tasks, improving personnel selection procedures, providing for self- and external checking, planning and scheduling to reduce time pressures and excessive fatigue, and providing positive incentives for high-quality performance can all be effective in reducing the incidence of HOE. The same problems must also be attacked at the organizational level, recognizing the important roles of organizational strategy, structure, communication, decision making, and culture in fostering the reduction of HOE.

We need to develop practical and realistic risk management procedures to integrate HOE considerations with system performance considerations. These procedures are needed to allow engineers, managers, and regulators to understand the potential nature of critical problems, how they might best be cured, and the costs and benefits of alternatives for cures. While these procedures might not be perfect, nor the data and information that is used to implement them complete, the process of performing the assessments can provide substantial benefits. The objective of the qualitative and quantitative procedures being developed in this research is not prediction; it is improved risk management of marine systems.

REFERENCES

Arrow, K. J. (1986). *Social Choice and Individual Values*. New York: Cowles Foundation and Wiley.

——— (1972). *Decision and Organization*. Amsterdam: North Holland Publications.

Bea, R. G. (1989). "Human and organizational error in reliability of coastal and ocean structures." *Proceedings of the Civil College Eminent Overseas Speaker Program*, Institution of Engineers, Australia.

Carson, W. G. (1982). *The Other Price of Britain's Oil: Safety and Control in the North Sea*. Oxford, England: Martin Robertson & Company Ltd.

Construction Industry Research and Information Association (1977). *Rationalization of Safety and Serviceability Factors in Structural Codes*. London: CIRIA Report 63.

Davidson, A. (1990). *In Wake of the* Exxon Valdez: *The Devastating Impact of the Alaska Oil Spill*. San Francisco: Sierra Club Books.

Heising, C. D., and W. S. Grenzebach (1989). "The *Ocean Ranger* oil rig disaster: A risk analysis." *Risk Analysis, 9*, (1), 55–62.

Howard, R. A. (1966). "Information value theory." *IEEE Transactions on Systems, Man, and Cybernetics, SSC-2*, (1), 22–26.

Ingles, O. G. (1985). "Human error, and its role in the philosophy of engineering." Doctoral thesis, University of New South Wales, Australia.

Kahneman, D., P. Slovic, and A. Tversky (1982). *Judgment Under Uncertainty: Heuristics and Biases*. New York: Cambridge University Press.

La Porte, T. R. (1988). High Reliability Organization Project. Berkeley: University of California.

Larocque, G. R., and K. Mudan, (1982). *Costs and Benefits of OCS Regulations: Volume 3—Preliminary Risk Analysis of Outer Continental Shelf Activities*. Cambridge, MA: Arthur D. Little, Inc.

Lord Cullen Report (1990). *The Public Inquiry into the* Piper Alpha *Disaster*. United Kingdom Department of Energy. London: HMSO Publications.

March, J. G., and H. A. Simon (1958). *Organizations*. New York: Wiley.

Melchers, R. E. (1976). *Societal Options for Assurance of Structural Performance*. London: Final Report, 11 Congr, IABSE.

——— (1987) *Structural Reliability Analysis and Prediction*. Brisbane, Australia: Ellis Horwood Limited, Halsted Press: A division of John Wiley & Sons.

Minerals Management Service OCS Report (1990). "Investigation of March 19, 1989, Fire *South Pass Block 60 Platform B* Lease OCS-G 1608." MMS 90-0016. Washington, D.C.: U.S. Department of Interior.

Moan, T. (1981). "The *Alexander Kielland* Accident." *Proceedings from the First Robert Bruce Wallace Lecture*, Department of Ocean Engineering. Boston: Massachusetts Institute of Technology.

——— (1983). "Safety of offshore structures." *Proceedings, Fourth International Conference on Applications of Statistics and Probability in Soil and Structural Engineering*.

National Bureau of Standards (1985) "Application of risk analysis to offshore oil and gas operations." *Proceedings of an International Workshop*, NSB Special Publications 695. Washington, D.C.: U.S. Department of Commerce.

National Transportation Safety Board (1987). Capsizing and Sinking of the United States Drillship *Glomar Java Sea* in the South China Sea 65 Nautical Miles South-Southwest of Hainan Island, Peoples Republic of China, October 25, 1983. Washington, D.C.: NTSB/MAR-87/02.

Nessim, M. A., and I. J. Jordan, (1985). "Models for human error reliability." *Journal of Structural Engineering, 111*, 6, 1358–1376.

Noreng, Ø. (1980). *The Oil Industry and Government Strategy in the North Sea*. London: Croom Helm.

Nowak, A. S. (1986). "Modeling human error in structural design and construction." *Proceedings of a Workshop Sponsored by the National Science Foundation*. New York: American Society of Civil Engineers.

Offshore Certification Bureau (1988). "Comparative safety evaluation of arrangements for accommodating personnel offshore." Report OTN-88-175.

Panel on Human Error in Merchant Marine Safety (1976). "Human Error in Merchant Marine Safety." Maritime Transportation Research Board Report. Washington, D.C.: National Academy of Sciences.

Paté-Cornell, M.E. (1986). "Warning systems in risk management." *Risk Analysis, 6*, 2, 223–234.

———(1990). "Organizational aspects of engineering system safety: The case of offshore platforms." *Science, 250*, 1210–1217.

Paté-Cornell, M. E. and R. G. Bea, (1989). "Organizational aspects of reliability management: Design, construction, and operation of offshore platforms." Research Report No. 89-1. Department of Industrial Engineering and Engineering Management. Palo Alto: Stanford University.

Paté-Cornell, M. E., and J. P. Seawell (1988). "Engineering reliability: The organizational link." *Proceedings of the ASCE Specialty Conference on Probabilistic Mechanics and Structural and Geotechnical Safety*, Blacksburg, Virginia.

Perrow, C. (1984). *Normal Accidents: Living with High Risk Technologies*. New York: Basic Books, Inc.

Reason, J. (1990). *Human Error*. New York: Cambridge University Press.

Reid, S. G. (1989). "Guidelines for risk based decision-making." Investigation Report No. S726, School of Civil and Mining Engineering. Sydney: The University of Sydney.

Roberts, K. H. (1992): "Top Management and effective leadership in high technology." In L. Gomez-Mehia and M. W. Lawless, (eds.), Vol. III. *Top Management and Effective Leadership in High Technology Firms*. Greenwich, CT: JAI Press.

Roberts, K. H., D. M. Rousseau, and T. R. La Porte (in press). "The culture of high reliability: Quantitative and qualitative assessment aboard nuclear powered aircraft carriers." *Journal of High Technology Management Research*.

Royal Commission on *Ocean Ranger* Marine Disaster (1985). Report of the Royal Commission of the *Ocean Ranger* Marine Disaster. Ottawa, Ontario, Canada.

Royal Norwegian Council for Scientific & Industrial Research (1979). Risk Assessment Report of the Norwegian Offshore Petroleum Activities. Oslo, Norway.

Shachter, R. D. (1986). "Evaluating influence diagrams." *Operations Research, 34*, 6, 1210–1222.

United Kingdom Department of Energy (1988). "*Piper Alpha* Technical Investigation: Further Report." London: Crown.

Veritec (1988). *The Worldwide Offshore Accident Data Bank (WOAD) Annual Reports through 1988*. Oslo, Norway.

Weick, K. E. (1987). "Organizational culture as a source of high reliability." *California Management Review, 29*, 112–127.

Wenk, E., Jr. (1986). *Tradeoffs: Imperatives of Choice in a High-Tech World*. Baltimore: The Johns Hopkins University Press.

International Offshore Mechanics and Arctic Engineering Conference
Safety and Reliability Symposium
Houston, Texas, February 1994
Paper No. OMAE 94-1272

RELIABILITY BASED EVALUATIONS OF HUMAN AND ORGANIZATION ERRORS IN REASSESSMENT & REQUALIFICATION OF PLATFORMS

Robert G. Bea and William H. Moore

Department of Civil Engineering and
Department of Naval Architecture & Offshore Engineering
University of California
Berkeley, California

ABSTRACT

This paper addresses the impact of *Human and Organization Errors* (HOE) on the reliability assessments of existing offshore platforms. It examines how quantitative *Probabilistic Risk Analyses* (PRA) can be used as a tool to help evaluate the impact of HOE management alternatives to improve the reliability of existing platforms. Consideration of HOE is an extension of traditional PRA with several new *layers* of evaluations. These layers include the individual operators on the platform and the organizations or groups of people that influence the performance of the system.

INTRODUCTION

Experience with a wide variety of marine systems including fixed offshore platforms indicates that incidents such as blowouts, fires and explosions, and collisions account for the vast majority of reliability problems (Figure 1). During the period 1980 to 1990, the average annual total loss rate for fixed offshore platforms was 0.14 % (worldwide) (Veritec, 1992). The severe damage rate (Figure 1, damage ≥ $ 2 millions U. S.) was 0.66 %. Problems with the structures accounted for less than 10 % of the causes of severe damage.

Given this background, the objective of this paper is to define how reliability engineering might best be used to help improve the situation. The first step toward this objective is to recognize that the majority of operating reliability problems can be reduced. The rates of their incidence can be decreased and their consequences can be reduced. This reduction becomes an important strategy in requalifying existing offshore platforms. The total risk can be managed so that it is equal to or less than when the platform was installed.

The second step is to recognize that the prevention of operating accidents is firmly founded in improving the reliability of the humans and organizations that design, construct and operate marine systems. The source of a majority (generally more than 80%) of high consequence accidents associated with marine systems such as offshore platforms can be attributed to compounded HOE (Bea, 1989; Pate-Cornell, Bea, 1989) More than 80% of these accidents are founded in problems that develop primarily during operations of these systems. Recent examples include the *Occidental Piper Alpha* North Sea platform explosions and fire (167 men killed), the *Odeco Ocean Ranger* capsizing off Newfoundland (84 men killed), and the *Alexander Kielland* failure in the North Sea (123 men killed).

Figure 2 summarizes results from a recent reassessment and requalification study of an existing platform located in Cook Inlet, Alaska (Bea, Landeis, Craig, 1992). The study addressed the likelihood of platform failure (catastrophic damage or complete loss) due to extreme environmental loadings induced by ice and earthquakes and due to operating accidents. The results of the study indicated that 75 % of the total probability of failure was due to operating accidents associated with drilling, workovers, and high pressure gas processing and production. This would indicate that available safety resources should be directed primarily toward reducing the major contributors to the potential operating accidents.

This discussion should not be interpreted as implying that there are no significant HOE involved in the design and construction of marine systems. There are and they have had important effects on the reliability of marine systems (Moan, 1981; 1993) The *Occidental Piper Alpha, Odeco Ocean Ranger, Alexander Kielland* , and *Sleipner A* platform sinking all had roots that were firmly founded in HOE in design and construction.

ACCIDENT ORIGINS

Human errors have been shown to be the basic cause of failures of many engineered systems (Heising, Grenzebacvh, 1989; Moan, 1981, 1983, Veritec, 1992, Wenk, 1986; Blockley, 1992; Rasmussen, et al., 1987; Dougherty, Fragola, 1988). In almost all cases, the initiating event can be traced to a catastrophic compounding of human and organizational errors (Report of the Royal Commission, 1985; Ingles, 1985; Nowak, 1986; Roberts, 1990; Paté-Cornell, Seawell, 1988; Perrow, 1984).

High consequence accidents resulting from HOE can be differentiated into those that occur in design, *construction* and *operation* phases of the marine system's life cycle. Accidents can be the result of improper design and construction of the system. For example, primary contributors to the capsizing of the *Alexander Keilland* were the lack of redundancy (design flaws) and cracks (maintenance oversights) in the structure (Moan, 1981, 1993). Design flaws originating in the finite element modeling and lack of appropriate review were primarily responsible for the sinking of the Sleipner A platform.

Accidents resulting from operations can be categorized into *societal* (cultural), *organizational*, *individual*, and *systems* (hardware, software) errors. Societal values can substantially influence the frequency of human and organizational errors. Expedient offshore development in the United Kingdom, resulting from economic crises of the 1960's and 1970's, led to limited safety regulation and significantly high rates of accidents (Carson, 1982; Nøreng, 1980).

Organizational structure has been found to impact on operational reliability for offshore platforms in previous studies (Bea, 1989; Paté-Cornell, Bea, 1989; Paté-Cornell, 1990). For example, errors in management decisions resulted in the loss of the *Odeco Ocean Ranger* (Report of the Royal Commission, 1985; Heising, Grenzebach, 1989) and the excessive loss of life aboard the drill ship *Glomar Java Sea* (82 men killed) (National Transportation Safety Board, 1987). Individual errors are those which are made by a single person which can contribute to an accident. The chain of events which led to the *Occidental Piper Alpha* accident were initiated by events leading from an unfinished maintenance job in the gas compression module (Department of Energy, 1988; United Kingdom Department of Energy, 1990; Moore, Bea, 1993).

Experience indicates that the influences of the organizations on the reliability of marine systems generally is the most pervasive of the human factor related causes of accidents. High reliability organizations inherently develop high reliability operators, systems, and operations (and vice versa). High reliability organizations generally focus on the long-term quality of production, not on the short-term quantity of production (Roberts, 1990).

The sources of organization errors can be placed into three general categories. The first is *upper level management.* The lack of appropriate resources and commitments to achieve reliability and the provision of conflicting goals and incentives (e.g. maintain production when it needs to be decreased to allow maintenance to be performed on the system) are examples of upper level management errors.

The second is *front line management*. Information filtering (make it look better than it really is, tell the boss what he wants to hear - good news), and redirection of resources to achieve production at the expense of safety are examples of font line management errors.

The third category is the design, construction, or operating *team*. (National Research Council, 1993). Team work in which there is an inherent and thorough process of checking and verification have proven to be particularly important (*if you find a problem, you own it until it is either solved or you find someone to solve it).* The lack of team work represented in poor communications between work shifts (ineffective permit to work systems) or between work teams and the platform control room have resulted in several major accidents (Dougherty, Fragola, 1988).

Errors can also be observed with human-system (equipment, structure, software or instructions manuals) interfacing, these are described as *system errors and procedure errors.* System errors can be attributed to design errors and result in an operator making improper decisions. Similarly, the procedures and guidelines provided to design, construct, or operate a system can be seriously flawed. System errors led to the loss of the ballast control aboard the *Odeco Ocean Ranger* (Report of the Royal Comission, 1985) and emergency system failure aboard the *Occidental Piper Alpha* (Moore, Bea, 1993). Appropriate *operating manuals* on how to interrupt potentially catastrophic sequences were almost totally lacking in both of these cases.

The external and internal environments can contribute to the error producing potential of the humans that design, construct, and operate marine systems. Ex-

ternal environmental factors such as darkness, extreme low temperatures, and extreme storms can exacerbate human error producing potentials. Similarly, internal environmental factors such as poor visibility, smoke, and intense motions can cause errors (National Research Council, 1993).

Given the foregoing, the human factors related hazards can be organized as summarized in Figure 3. There are error producing potentials within each of the primary areas including the human operators (designers, constructors, operators), the organizations that influence these operators, the systems themselves (hardware), the documentation that embody the manuals of use or practice for the systems (software), and finally the external and internal environments. In addition to the error producing potentials within each of these areas, there are error producing potentials at the interfaces.

A detailed study of the present databases on marine accidents indicates that they are very deficient in their ability to accurately define the human factors involved in the marine accidents (Moore, Bea, 1991). There has not been any common classification or definition of human factor related causes. There has been a dearth of well trained accident investigators. Investigations generally have focused on the immediate causes of accidents, not the underlying factors that lead to these causes. Investigations have frequently been focused on placing blame rather than on determining the underlying, direct, and contributing factors that resulted in the accident. Organizational factors have largely been ignored. Due to legal action concerns, there is not a single generally available database that addresses violations related causes of marine accidents.

There is not a single available database that addresses the very important *near misses*. Inclusion of such information in operating databases could help indicate how operating personnel are able to interrupt potentially catastrophic compounding sequences of problems and bring the system back to a safe condition. If employed on "real time" basis, such information could provide very important early warnings of developing problems with operating systems.

Thus, the information that is available in present marine accident databases can only be used for very general purposes. This leaves the reliability analysts with three other ways to provide the necessary quantifications: 1) expert judgment, 2) laboratory simulations, and 3) field experiments (National Research Council, 1990). The author is aware of only one simulator that has been developed and employed to help train and evaluate platform operating personnel. Because this system is so new (placed in operation in 1993) there have not been any systematic studies or results developed as of this time. The author has not been able to locate a single field study that has been performed onboard a platform to develop HOE related data.

Given this situation, the only remaining option at this time is to utilize expert judgment backgrounded with adequate experience and the available information on accidents. Qualified expert opinion must be combined with the available data to provide quantifications that are required for analyses (National Research Council, 1990). The results of the analyses are dependent on the judgment and background that is integrated into the analyses. The purpose of the analyses must shift from prediction to assessments intended to identify potential critical flaws and evaluations of alternatives to minimize such flaws and reduce their impacts to acceptable levels.

HUMAN ERRORS

Based on an extensive study of available accident databases on marine systems (Moore, Bea, 1991) the primary factors which can result in human errors are identified in Figure 4. The errors range from those of judgment to *ignorance, folly, and mischief* (Wenk, 1986; Perrow, 1984). The sources of mistakes (cognitive errors) can be further defined as summarized in Figure 5 (Blockley, 1992).

These errors are magnified and compounded in times of crisis (National Research Council, 1993). Human performance levels vary between individuals depending upon training, variability between individuals, organizational pressures, and complexity of the operating system. Nevertheless, performance is observed to deteriorate when pressure levels are either too low or high (Melchers, 1976). For example, times of high pressures could be affected by stress or panic while low human performances could be the result of boredom. Both extremes can contribute to increase the incidence of human errors.

A mishap (Figure 6) can be differentiated into three psychological stages: *perceiving*, *thinking*, and *acting*. The danger threshold could be reached by either a lack of sufficient time to react, or errors in perception, thought or action which would either lengthen the time between events or increase the magnitude of the danger buildup. The perception stage starts with a mishap and is followed by a warning signal. The warning is then noticed and leads to recognition of the mishap source. The thinking stage begins with the identification of the problem and information (whether complete or incomplete) is processed at this stage to evaluate decisions for the best course of action. The mishap is acted upon with execution of a plan and the system is returned to a normal operating status or escalates to a dangerous state. Personnel selection and *crisis* training can have marked influences on an individ-

ual's ability to return the system to a safe state. *Near misses* are the result of such actions.

ORGANIZATION ERRORS

Organization error is a departure from acceptable or desirable practice on the part of a group of individuals that results in unacceptable or undesirable results. A summary of the principal factors that can contribute to or result in organization errors is given in Figure 7.

The analysis of past decisions regarding the operations of offshore platforms provides numerous examples of instances in which organizational failures have resulted in failures of marine systems (Bea, 1989; Paté-Cornell, Bea, 1989; Paté-Cornell, 1990). Either collections of individuals (organizations, societies) or individuals (unilateral actions) contribute to accident situations. Failures can occur as a result of an organization's or an individual's willingness to take a calculated risk. Failures can result from different types of inevitable errors that can be corrected in time, provided they are detected, recognized as errors, and corrective action is promptly taken.(Figure 6). Failures can also occur as the result of errors or bad decisions, most of which can be traced back to organizational malfunctions.

The goals set by the organization may lead rational individuals to conduct operations aboard a platform in a manner that corporate management would not approve if they were aware of their reliability implications (Howard, 1966; Kahneman, et al, 1982; Roberts, 1990). Similarly, corporate management, under pressures to reduce costs and maintain schedules, unknowingly may not provide the necessary resources required to allow adequately safe operations.

Generally, two classes of problems face an organization in making collective decisions that result from sequences of individual decisions: *information* (who knows what and when?), and *incentive* (how are individuals rewarded, what decision criteria do they use, how do these criteria fit the overall objectives of the organization?) (Arrow, 1972,; 1986; La Porte, 1988; National Research Council, 1990). In development of programs to improve management of HOE, careful consideration must be given to information (collection, communications, and learning) and incentives, particularly as they affect the balancing of several objectives such as costs and safety under uncertainty in operations of offshore platforms (Wenk, 1986; Weick, 1987).

The structure, the procedures, and the culture of an organization contribute to the safety of its product (Kahneman, et al., 1982; National Research Concil, 1990; Roberts, 1990) and to the economic efficiency of its risk management practices (Wenk, 1986; Royal Norwegian Council for Scientific and Indusrial Research, 1979). The organization's structure can be unnecessarily complex and demand flawless performance. This can result in little or no credible feedback to the upper levels of management. The resulting safety problem is that there may be inconsistencies in the decision criteria (e.g. safety standards) used by the different groups for various activities. This can result in large uncertainties about the overall system safety, about the reliability of the interfaces, and about the relative contribution of the different subsystems to the overall failure probability (Moan, 1981; 1993; Construction Industry Research and Information Association, 1977; National Bureau of Standards, 1985).

Organization and management procedures that affect system reliability include, for example, parallel processing such as developing design criteria at the same time as the structure is being designed, a procedure that may or may not be appropriate in economic terms according to the costs and the uncertainties (Paté-Cornell, 1990).

The culture of the organization can also affect system reliability (Wenk, 1986; Arrow, 1972; 1986; Reason, 1990; Perrow, 1984; Roberts, 1990). For example, the dominant culture may reward risk seeking (flirting with disaster) or superhuman endurance (leading to excessive fatigue), an attitude that in the long run may prove incompatible with the objectives of the organization. Another feature may be the lack of recognition of uncertainties leading to systematic biases towards optimism and wishful thinking (Paté-Cornell, Seawell, 1988).

SYSTEM ERRORS

Errors can also be exacerbated by poorly engineered systems that invite errors. In this context, the term systems is taken to include both the hardware and the software. Such systems are difficult to construct, operate, and maintain (Ingles, 1985; Melchers, 1987; Moan, 1981, 1993).

New technologies compounds the problems of latent system flaws. Complex design, close coupling (failure of one component leads to failure of other components) and severe performance demands on systems increase the difficulty in controlling the impact of human errors even in well operated systems (Perrow, 1984). Emergency displays have been found to give improper signals of the state of the systems (Heising, Grenzebach, 1989; Lord Cullen Report, 1990; Perrow, 1984; National Research Council, 1993). Land based industries can spatially isolate independent subsystems whose joint failure modes would constitute a total system failure. System errors resulting from complex designs and close coupling are

more apparent due to spatial constraints aboard platforms. For example, spatially and environmentally isolating the control room and accommodations unit on *Piper Alpha* could have substantially reduced the loss of life aboard the platform (82 men died in the accommodations unit) (United Kingdom Dept. of Energy, 1990).

Human performance is a function of the lead time available to respond to warnings in the system (Figure 6). Errors are compounded by the lack of effective early warning systems (Paté-Cornell, 1986). If the lead time is short, there is little time allowance for corrective action before the situation reaches a critical state. On the other hand, if the system is too sensitive resulting in frequent false alarms, operators will eventually cease to respond to the warning signals. The time differential between the normal and warning stages are dependent upon the sensitivity of the system to developing danger. Human performance is critical in the initiation of the alert stage (warning) and an expedient execution of a plan (corrective action) brings the system back under control (National Research Council, 1993).

PROBABILISTIC RISK ANALYSIS WITH HOE

If HOE affect a subsystem whose functioning is not highly critical, their effect on the overall system reliability may be minor and not justify profound human or system changes. However, complex interactions of relatively independent subsystems can substantially affect overall system reliability due to system complexities and tight coupling (Perrow, 1984). If deficiencies affect a subsystem or a complex interaction of subsystems whose failure constitutes a system failure mode, it is urgent to address the problem at its human and system origins To permit evaluations of the interactions of the human and system components, it is desirable to organize and assess these features in a *Probabilistic Risk Analysis* (PRA) (Moan, 1993). This allows one to develop insights into the urgency of remedial measures, to evaluate alternative remedial measures to improve safety, and to set priorities among HOE problems to be addressed.

A PRA for engineering systems allows identification of the weakest parts of a system through qualification of the probabilities of the different failure modes. Event tree modeling (Howard, Matheson, 1981; Schachtger, 1986), a form of PRA, has been found to be an effective method to analyze contributions of individual accidents to risk associated with offshore operations (Moore, Bea, 1993). This technique permits setting priorities among possible modifications aimed at the reduction of the failure risks and, therefore, optimal allocation of limited risk management resources.

The general method is to integrate elements of process analysis of the system hardware and software and human individual and organizational analysis in the assessment of the probability of system failure (Figure 3). The first phase is a preliminary PRA to identify the key subsystems or elements that can have important effects on the system's reliability. The second phase is an analysis of the process to identify the potential problems for each of the subsystems and their probabilities or base rates per time unit or per operation.

Given that a basic error occurs, the next phase is an analysis of the organization and individual operator system to determine their influence on the occurrence of basic errors and the probability that they are observed, recognized, communicated, and corrected in time (i.e., before they cause a system failure) (Figure 6).

The result of these three phases is a computation of the probabilities of the different systems' states corresponding to possible types of system defects and, therefore, to different levels of the system's capacity. The fourth phase involves a return to the PRA for the physical system and a computation of the probability of failure for each capacity level corresponding to the different system states.

The overall failure probability is then obtained. It explicitly includes the possibility of weaknesses in the different subsystems due to human and organizational components. These different models (process, human, organization, and final PRA) are integrated using event trees or influence diagrams to compute the failure probabilities under different circumstances (e.g., occurrence and correction of a given problem in the process).

One can quantify the costs and benefits of HOE reliability management measures using PRA (Nessim, Jordaan, 1985; Larocque, Mudan, 1982). The analysis of a system's reliability allows identification of its failure modes and computation of their probabilities. It permits a decision maker to choose technical solutions that maximize an objective function (costs and reliability) under resource constraints (Wenk, 1986; Construction Industry Research and Inforemation Association, 1977). These solutions include, for instance, the choice of operating procedures and equipment that minimize the probability of failure during the lifetime of a structure under constraints of safety budgets, costs, time to completion, production level, structure location and general type. The results of the analysis can provide valuable insights into where scarce safety resources can best be deployed to achieve the largest improvements in safety.

A probabilistic model of the process includes determining the set of possible initiating accident events (in_i) and final states ($fist_m$) of the system. The probability of

loss of components (platform, vessel, revenue, life, injury, etc.) to the system can then be represented by:

$$p(loss_k) = \sum_i \sum_m p(in_i)\ p(fist_m|in_i)\ p(loss_k|fist_m) \quad (1)$$

(" k: "for all values of k")

The model is expanded to include relevant decisions and actions (A_n) constituting an exhaustive and mutually exclusive set of decisions or actions affecting the marine system at different stages during a given period of the platform life (e.g. annual). These decisions and actions can be examined from the front-line operating crew level through to top-level management.

$$p(loss_k) = \sum_i \sum_m \sum_n p(A_n)\ p(in_i|A_n)\ p(fist_m|in_i, A_n) \quad (2)$$

The effects of organizational procedures and policies on the risk are determined through examining the probabilities of the actions and decisions conditional on relevant organizational factors (O_h). The probabilities of various degrees of loss can be examined conditional upon different contributing organizational factors.

$$p(loss_k|O_h) = \sum_i \sum_m \sum_n p(A_n|O_h)\ p(in_i|A_n)\ p(fist_m$$

(3)

INFLUENCE DIAGRAMS

One method of developing accident framework models for PRA analysis is through the use of *influence diagrams*. Influence diagramming is a form of PRA modeling which allows greater flexibility in examining HOE and HOE management alternatives. There are distinct advantage for using influence diagramming as an alternative to standard event/fault tree analyses. Influence diagrams are used to organize conditional probability assessments required to determine unconditional probabilities of failures of specified target events. In standard decision tree analysis, decisions are based on all preceding aleotory and decision variables. However, not all information is necessarily available to a decision maker. In addition, information may come from indirect sources or not the specific order in which the decision tree is modeled. It is not necessary for all nodes be totally ordered in an influence diagram. This allows for decision makers who agree on common based states of information, but differ in ability to observe certain variables in the diagram modeling (Schachtger, 1986; Howard, Matheson, 1981).

As described by Howard and Matheson (1981) the components of an influence diagram are: (1) *decision* and *chance nodes*, (2) *arrows*, (3) *deterministic nodes*, and (4) *value nodes* Decisions are represented by square nodes which can be a continuous or discrete variable or set of decision alternatives. Uncertain events or variables are represented by circular or oval chance nodes. Chance nodes can be continuous or discrete random variables or a set of events. Arrows indicate relationships between nodes in the diagram. Arrows entering a chance node signify that the probability assignments of the node are conditional upon the node from which the arrow originated. Deterministic nodes are those in which outcomes depend deterministically upon its predecessors. A value node is designated by the author to be: "the quantity whose certain equivalent is to be optimized by the decisions" of which only one node may be designated in the diagram. These nodes are represented by a rounded edge double-border rectangle. A description of influence diagrams are discussed in Howard & Matheson (1981).

To establish the set of events which have occurred in a specific accident sequence, the modeler may wish to construct a preliminary influence diagram representation of the accident. The preliminary model representation is not an influence diagram per se, but a representation of the specific events, actions, and decisions which occurred during the accident event. The purpose of the preliminary model is to assist the user in establishing the relevant contributing factors unique to the specific accident sequence. No probabilistic assessments are made from the preliminary model. In addition, it can assist the user in identifying critical areas where: (1) further detailed studies may be warranted, or (2) if properly managed or controlled, could have reduced the risk or consequences of the accident.

As shown in Figure 8 the modeling process begins with a specific accident model formulation and results in the development of an influence diagram model for a particular class of accidents. The influence diagram models encompass the class of accidents in which the post-mortem model is a representative. The development of influence diagram models (and preliminary model representations) should be the effort of a group of experts. Discussion of differences in opinion of relationships between events and their causes illicit the development of more realistic models. The models are developed through an iterative process discussed between experts to determine relevant influences and correlations between subsystems and operations.

The modeling process includes the structuring of a target event (e.g. loss of high pressure gas containment on the platform) which is the final result of contributing events, decisions, and actions. The first step is to develop

a model representing dependencies between relevant events. Events can be categorized into three states:

(1) *Contributing/underlying events*: The set of events which lead to an initiating accident event. Contributing/underlying events are those occurring prior to the initiating accident event contributing to the reduction of reliability or increase of risk for the system. For example, simultaneously producing and conducting production process maintenance (*Piper Alpha*).

(2) *Initiating/direct accident events*: The immediate accident event(s) resulting in the casualty. For example, the initial explosions aboard a production platform subsequently lead to a compounding of events (e.g. loss of life and platform).

(3) *Compounding events*: The progression of events which lead to compounding of accident consequences. For example, increasing the flow of gas from satellite platforms (*Claymore* and *Tartan* to *Piper Alpha*) thus escalating the fire (Moore, Bea, 1993).

One of the keys to the development of an effective models is to determine the goals, preferences, and needs of the ultimate user of the results. For example, offshore platform operators may wish to establish models that enable them to focus on specific areas to allocate limited resources. These goals and preferences may be established in the model to examine the effects of the operating alternatives as the driving force by balancing safety, economic, and production costs and benefits. On the other hand, regulators and policy makers may wish to establish environmental, economic and social risks and costs of specific types of offshore operations. In short, the models should be varied in extent and detail to reflect the preferences of the user in examining costs and benefits of these operations.

The complexity of the model must be weighed against the time, available resources, goals and preferences of the user. A primary issue in model development is striking a balance between a general models or highly detailed examinations of specific operations. The users must ask themselves if the marginal value of information gained as the model being constructed becomes more complex worth the additional input of resources. For example, the user may wish to establish a general framework model with only limited detail and spend more time on analysis and examining the effects of sensitivity and uncertainty in the model. Yet another individual or group may wish to develop a detailed model at a substantial cost in time and resources. This preference allows the user to examine detailed aspects of human performance or limit the level of ambiguity and uncertainty in the model.

Regardless of the level of detail in which the modeler may wish to include, each model begins with a *template* diagram which forms a basis for a specific operation (Moore, Bea, 1993). The template is a diagram involving the most relevant factors affecting a class of accidents or specific operation. The development of a model diagram is cyclic process. The preliminary model diagram can be used to construct a general template. Development of a model are an iterative process. The structure of the model should be shown to key players in the operation (managers, front line operators, regulators, consultants, etc.) to discuss whether the models are consistent with their judgments and experiences. If results are not consistent with case history examples and general quantitative measures, further refinements should be made.

EXAMPLE: GAS DETECTION ALTERNATIVES

Using the influence diagram shown in Figure 8, one can consider two alternatives for emergency gas detection and shutdown in a platform compression module. Alternative 1 - manual monitoring of the compressor module by an operator on duty around the clock, and Alternative 2 - installing an emergency gas detection and shutdown system which is operated from the platform control room. These alternatives are examined to determine the eventual failure probabilities of the power plant resulting from fires initiated by compression module gas leaks.

Each single border oval or circular node shown in Figure 8 describes probabilistic nodes while double border nodes describe deterministic values in the model. Based on available accident data involving compressor system leaks, Table 1 summarizes the probabilities of a gas leak in the compression module.

A probability distribution is established for the magnitude of the leak and is represented by the *leak size* node. Again, based on available statistics concerning loss of containment in compression modules, Table 2 summarizes this probability distribution for leak sizes. The leak size will influence three factors: (1) the detection of gas, (2) the magnitude of the fire, and (3) location of an ignition source. Gas detection is dependent upon its concentration in the ambient atmosphere around either the compression module operators (detection by smell, sound, or gauging) or the automatic gas detection system (GDS). Gas detection is a step process for both manual and automatic operations: a warning signal followed by the problem recognition, identification, and execution of a plan (Figure 6). The larger the leak, the greater the chance of detection. Table 3 summarizes the conditional probability distribution for gas detection dependent upon the initiation of the leak and its size. It is here that the reliability of the human and system detection

components must be assessed. In addition, the gas must locate an ignition source for a fire to be initiated. The model assumes the greater the magnitude of the gas leak, the greater the probability it finds an ignition source as shown in Table 4.

The *proper course of action?* node models whether operators were able to return the system to a normal state by intervening to prevent the fire from occurring. The distributions shown in Table 5 demonstrate two factors that are indicated by present data on containment of gas leaks in gas compression modules: (1) the probability of manual control of a leak or fire is greater than that of automatic control since both manpower and mechanical expertise are available to extirpate the problem, and (2) passive monitoring from the platform control room can lead to a limited alert time before escalation to a state which can be extremely difficult to control.

As shown in Figure 8, fire initiation, presented by the deterministic node *fire*, is dependent upon three factors: (1) if the gas was detected, (2) whether a proper course of action was carried out to control the leak if detected, and (3) if the gas encountered an ignition source. Table 6 shows the conditions in which a fire event occurs.

As represented in Figure 8, *fire magnitude* is dependent upon both the size of the leak and fire occurrence. The larger the gas leak, the greater the chance of a larger magnitude fire. These assumptions are represented by the probabilistic distributions shown in Table 7.

Finally, due to the proximity of the compression module to the main processing module, the magnitude of the fire will have an affect on the probability of failure of the platform's power plant. The fire events represented by the fire magnitudes will determine whether the power plant is operational. It is assumed that if the fire events are small, they can be effectively controlled and do not pose a threat to the integrity of the power plant. If the fire is moderate or large, the integrity of the power plant is affected and the plant fails (this may be due to heat, smoke, or flame moving from the pump room to the engine room).

Based upon the assumptions of the probabilistic and deterministic variables discussed above, Table 8 summarizes both the failure probabilities of the power plants and the conditional failures of the power plants dependent upon fire events. Though the automatic GDS is better at detecting gas leaks than human operators, the probabilities of fires for the manual system are approximately half those of the GDS system. This is primarily the result of the limited ability to control a fire due to limited manpower. Similarly, the probabilities of plant failures for the automated system are approximately twice that of the manual system.

CONCLUSIONS

In traditional reliability based studies of marine systems, HOE has been implicitly integrated into the background of accident statistics and experience on which such studies are often based. The principal focus of these studies has been the structural aspects or the equipment aspects, and how the design might be improved to improve reliability.

In recent times, engineers have come to recognize that they may have been working on only a small part of the problem of the reliability of marine systems. Given that some 80% of major accidents can be directly traced to HOE, it would seem appropriate that engineers would begin to explicitly evaluate how marine systems and the humans that are an integral part of these systems from their design to their decommissioning can be better configured to improve safety.

Experience indicates that the majority of high consequence, low probability marine accidents have one common theme: *a chain of important errors made by people in critical situations involving complex technological and organizational systems. Many of these errors involve fatigue, carelessness, negligence, short sightedness, greed, lack of training, and wishful thinking.*

The errors go beyond individuals directly involved in the incidents. There are organizations that provide *cultures* that invite excessive risk taking, demanding superhuman performance, and developing complacency that results in reactive risk management. Short sightedness, with a central focus on present profitability seems to be a primary factor in such cultures. Industry, government, and society all share in providing such cultures.

In some cases, engineers have been designing marine systems that cannot be constructed and operated as they should, so field modifications and short-cuts must be developed. The engineer rarely hears about these problems, until they become critically evident. People are transferred so rapidly and in some cases retired so early that there is a loss of corporate memory of these mistakes. Unnecessary complexity in systems (physical and organizational) invites errors. When one engineers an overly complex system, and places it in the hands of improperly trained, motivated, and verified people, then one is asking for the trouble we have been experiencing.

The human and organizational elements of marine systems must be engineered and designed, just as the physical elements of these systems, are engineered and each of these need to compliment the other. Engineers must learn how to design systems to be more forgiving and tolerant of errors and flaws; people tolerant systems. Those responsible for the reliability and safety of marine

systems must honestly recognize the potential blindness produced by pride, wishful thinking, physical limitations (fatigue, boredom, confusion, ignorance), reckless ways (drug abuse, greed, lack of integrity), and the differences between what we know we should do and what we actually will do.

The HOE problem must be attacked at the level of the individual; training, testing, motivating, and verifying to a degree commensurate with the job to be performed and the needs for safety in the job. People must be trained how to manage crisis situations in the systems they operate. Reduction in complexity of tasks, improvements in personnel selection procedures, providing for self and external checking, planning and scheduling to reduce time pressures and excessive fatigue, and providing positive incentives for high quality performance can all be effective in reducing the incidence of HOE.

Engineers need to develop and impliment practical and realistic risk management procedures that will integrate HOE considerations with system performance considerations. These procedures are needed to allow engineers, mangers, and regulators to understand the potential nature of critical problems, how they might best be cured, and the costs and benefits of the alternatives for cures. While these procedures might not be perfect, nor the data and information that is used to implement the procedures be complete, the process of performing the assessments can provide substantial benefits. The primary objective of the procedures advanced in this paper is not prediction; the primary objective is improved risk management of existing platforms.

REFERENCES

Arrow, K. J., 1972, **Decision and Oganization,** North Holland Publications: Amsterdam.

Arrow, K. J., 1986, **Social Choice and Individual Values,** New York, Cowles Foundation and Wiley.

Bea, R.G., 1989, "Human and Organizational Error in Reliability of Coastal and Ocean Structures.," **Proceedings of the Civil College Eminent Overseas Speaker Program,** Institution of Engineers, Australia.

Bea, R.G., Landeis, B.T., Craig, M.J.K., 1992, "Requalification of a Platform in Cook Inlet, Alaska," POroceedings of the Offshore Technology Conference, OTC 6935, V. 2, pp. 551-562.

Blockley, D. (Ed), 1992, **Engineering Safety,** McGraw-Hill Book Company, London.

Carson, W.G., 1982, **The Other Price of Britain's Oil: Safety and Control in the North Sea,** Martin Robertson & Company Ltd., Oxford, England.

Committee on Human Factors, 1990, **Distributed Decision Making,** Commission on Behavioral and Social Sciences and Education, National Research Council, National Academy Press, Washington, DC.

Committee on Human Factors, 1990, **Quantitative Modeling of Human Performance in Complex, Dynamic Systems,** S. Baron, D. S. Kruser, and B. M. Huey (editors), Commission on Behavioral and Social Sciences and Education, national Research Council, National Academy Press, Washington, DC.

Construction Industry Research and Information Association, 1977, Rationalization of Safety and Serviceability Factors in Structural Codes, London, England: **CIRIA Report 63.**

Dougherty, E. M. Jr., Fragola, J. R., 1988, **Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications,** John Wiley &Sons, New York.

Heising, C.D., and Grenzebach, W.S., 1989, "The *Ocean Ranger* Oil Rig Disaster: A Risk Analysis," **Risk Analysis,** 9(1).

Howard, R. A., 1966, Information Value Theory, **IEEE Transactions on Systems, Man, and Cybernetics,** Vol. SSC-2 (1) 22-26.

Ingles, O.G., 1985., **Human error, and Its Role in the Philosophy of Engineering,** Doctoral Thesis, University of New South Wales, Australia.

Kahneman, D., Slovic P., & Tversky, A., 1982., **Judgment Under Uncertainty: Heuristics and Biases,** New York: Cambridge University Press.

La Porte, T.R., 1988, **High Reliability Organization Project,** Berkeley: University of California.

Larocque, G. R. & Mudan, K., 1982. **Costs and Benefits of OCS Regulations: Volume 3- Preliminary Risk Analysis of Outer Continental Shelf Activities,** Arthur D. Little Inc. Cambridge, MA.

Lord Cullen Report, 1990, **The Public Inquiry into the *Piper Alpha* Disaster,** United Kingdom Department of Energy, HMSO Publications, London.

March, J. G. & Simon, H.A., 1958, **Organizations,** New York: John Wiley & Sons.

Melchers, R.E., 1987, **Structural Reliability Analysis and Prediction,** Brisbane, Australia: Ellis Horwood Limited, Halsted Press: a division of John Wiley & Sons.

Moan, T., 1981. The Alexander Kielland Accident. **Proceedings from the First Robert Bruce Wallace Lecture**, Department of Ocean Engineering, Massachusetts Institute of Technology.

Moan, T., 1993, "Reliability and Risk Analysis for Design and Operations Planning of Offshore Structures," Proceedings of Sixth ICOSSAR, Innsbruck, Balkema Publishers, Rotterdam.

Moore, W. H., Bea, R. G., 1991, **Human and Organizational Error in Marine Systems: A Review of Existing Taxonomies and Databases,** Research Report No. 91-1, Dept. of Naval Architecture and Offshore Engineering, University of California, Berkeley.

Moore, W. H., Bea, R. G., 1993, "Human and Organizational Error in Operations of Marine Systems: Occidental Piper Alpha," Proceedings of the Offshore Mechanics and Arctic Engineering Conference, Vol. II, Glasgow, Scotland, ASME.

National Bureau of Standards 1985. Application of Risk Analysis to Offshore Oil and Gas Operations, **Proceedings of an International Workshop, NSB Special Publications 695.** U.S. Department of Commerce: Washington, D.C.

National Transportation Safety Board 1987. **Capsizing and Sinking of the United States Drillship *Glomar Java Sea* in the South China Sea 65 Nautical Miles South-Southwest of Hainan Island, Peoples Republic of China, October 25, 1983.** NTSB/MAR-87/02.

Nessim, M.A. & Jordaan, I.J., 1985, "Models for Human Error Reliability, **Journal of Structural Engineering,** 111(6).

Noreng, Ø., 1980. **The Oil Industry and Government Strategy in the North Sea,** Croom Helm, London.

Nowak, A.S., 1986, Modeling Human Error in Structural Design and Construction, **Proceedings of a Workshop Sponsored by the National Science Foundation, American Society of Civil Engineers.**

Offshore Certification Bureau, 1988, **Comparative Safety Evaluation of Arrangements for Accommodating Personnel Offshore.** Report OTN-88-175.

Panel on Workload Transition, Committee on Human Factors, 1993, **Workload Transition: Implications for Individual and Team Performance,** B. M. Huey and C. D. Wickens (editors), Commission on Behavioral and Social Sciences and Education, national Research Council, National Academy Press, Washington, DC.

Paté-Cornell, M.E., 1986, "Warning Systems in Risk Management," **Risk Analysis**, Vol. 6, No.2.

Paté-Cornell, M.E., 1990, "Organizational Aspects of Engineering System Safety: The Case of Offshore Platforms," **Science,** Vol. 250, pp. 1210-1217.

Paté-Cornell, M.E. & Bea, R.G., 1989, **Organizational Aspects of Reliability Management: Design, Construction, and Operation of Offshore Platforms,** Research Report No. 89-1, Department of Industrial Engineering and Engineering Management, Stanford University.

Paté-Cornell, M.E. and Seawell, J.P., 1988., "Engineering Reliability: The Organizational lLnk," **Proceedings of the ASCE Specialty Conference on Probabilistic Mechanics and Structural and Geotechnical Safety,** Blacksburg, Virginia.

Perrow, C., 1984, **Normal Accidents: Living with High Risk Technologies,** New York: Basic Books, Inc.

Rasmussen, J. , Duncan, K., and Leplat, J. (Ed.), 1987, **New Technology and Human Error,** John Wiley & Sons, New York.

Reason, J., 1990, **Human Error**, Cambridge University Press: New York, New York.

Roberts, K.H., 1990, "Top Management and Effective Leadership in High Technology, Prepared for **L. Gomez-Mehia & M. W. Lawless (Eds.) (vol. III). Research series on managing the high technology firm**. Greenwich, CT: JAI Press.

Royal Commision on *Ocean Ranger* Marine Disaster , 1985, **Report of the Royal Commission on the *Ocean Ranger* Marine Disaster.** Ottawa, Ontario, Canada.

Royal Norwegian Council for Scientific & Industrial Research, 1979, **Risk Assessment Report of the Norwegian Offshore Petroleum Activities,** Oslo, Norway.

Schachtger, R.D., 1986, Evaluating Influence Diagrams., **Operations Research,** Vol. 34, No. 6.

United Kingdom Department of Energy, 1988, **Piper Alpha Technical Investigation: Further Report.** Crown: London.

Veritec, 1992 **The Worldwide Offshore Accident Data Bank (WOAD).** Annual Reports through 1992 Oslo, Norway.

Weick, K.E., 1987, "Organizational Culture as a Source of High Reliability, **California Management Review,** Winter,.

Wenk, E., Jr., 1986, **Tradeoffs, imperatives of Choice in a High-Tech Worldm** The Johns Hopkins University Press.

TABLE 1. PROBABILITY OF PUMP MODULE GAS LEAK

Gas Leak (GL)	0.005
No Gas Leak (NGL)	0.995

TABLE 2. PROBABILITIES OF PUMP MODULE GAS LEAK SIZES

Small Leak (SL)	0.70
Moderate Leak (ML)	0.25
Large Leak (LL)	0.05

TABLE 3. PROBABILITIES OF PUMP MODULE GAS LEAK DETECTION BEFORE IGNITION

Leak Condition	Leak Size	Leak Detection	Probability of Detection With Automatic Gas Detection System (GDS)	Probability of Detection With Module Manual Operators
Leak	Small	Yes	0.90	0.75
		No	0.10	0.25
	Medium	Yes	0.99	0.85
		No	0.01	0.15
	Large	Yes	0.999	0.95
		No	0.001	0.05
No leak	No leak	Yes	0.00	0.00
		No	1.00	1.00

TABLE 4. PROBABILITIES OF GAS LEAKS IGNITING

Leak size	Ignition Source Located	Probability of Ignition
Small	Yes	0.4
	No	0.6
Medium	Yes	0.7
	No	0.3
Large	Yes	0.95
	No	0.05
No leak	Yes	0.00
	No	1.00

TABLE 5. PROBABILITIES OF EXTINGUISHING GAS LEAK FIRE

Gas Detection	Leak Controlled	Probability Using Manual Operation	Probability Using GDS System
Yes	Yes	0.90	0.60
Yes	No	0.10	0.40
No	No	1.0	1.0

TABLE 6. CONDITIONS TO INITIATE FIRE

Ignition Source Located ?	Leak Controlled ?	Gas Detected ?	Fire Event
Yes	Yes	Yes	No fire
Yes	No	Yes	Fire
Yes	No	No	Fire
No	Yes	Yes	No fire
No	No	Yes	No fire
No	No	No	No fire

TABLE 7. PROBABILITY DISTRIBUTION OF FIRE MAGNITUDES

Leak Size	Fire Event	Fire Magnitude	Probability of Fire Magnitude
No leak	Fire	No fire	1.0
	No fire	No fire	1.0
Small	Fire	Small	0.75
	Fire	Moderate	0.175
	Fire	Large	0.075
	No fire	No fire	1.0
Medium	Fire	Small	0.25
	Fire	Moderate	0.5
	Fire	Large	0.25
	No fire	No fire	1.0
Large	Fire	Small	0.2
	Fire	Moderate	0.4
	Fire	Large	0.4
	No fire	No fire	1.0

TABLE 8. PROBABILITIES OF MODULE FAILURE FOR OPERATIONAL ALTERNATIVE

Manually Operated System	Probabilities of Failure (annual)
Fire	7.58×10^{-4}
Plant Failure	3.11×10^{-4}
Automatic Gas Detection System	
Fire	1.33×10^{-3}
Plant Failure	6.19×10^{-4}

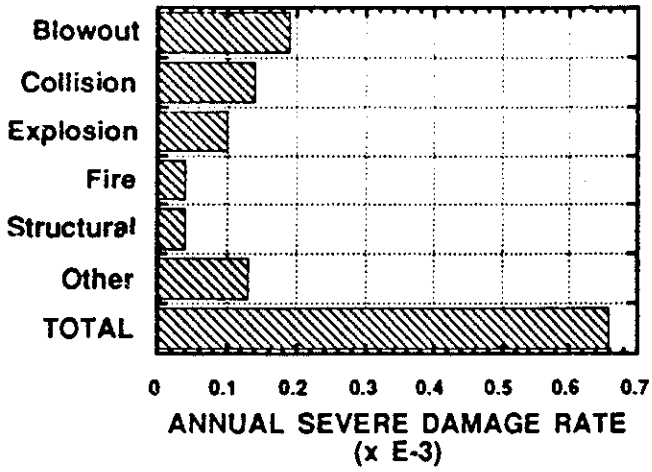


FIGURE 1. INITIATING EVENTS LEADING TO SEVERE DAMAGE TO FIXED PLATFORMS (1980 - 1990)

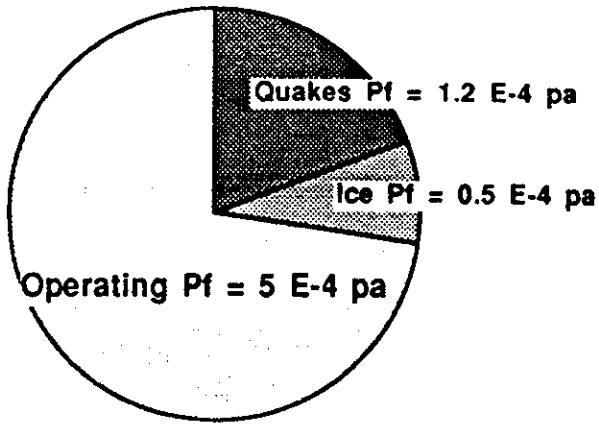


FIGURE 2. NOTIONAL ANNUAL PROBABILITIES OF FAILURE FOR COOK INLET PLATFORM

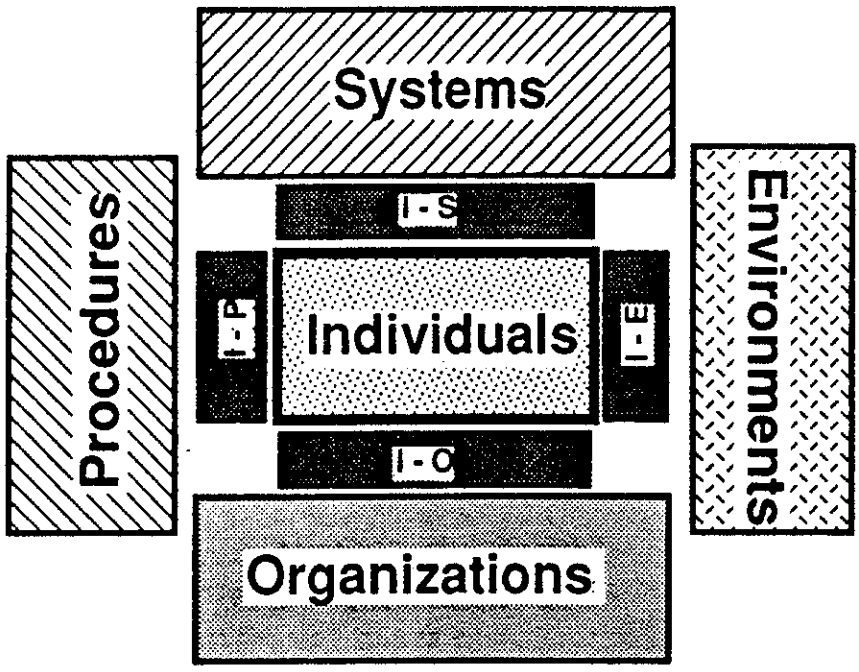


FIGURE 3 - HUMAN ERROR COMPONENTS AND INTERFACES

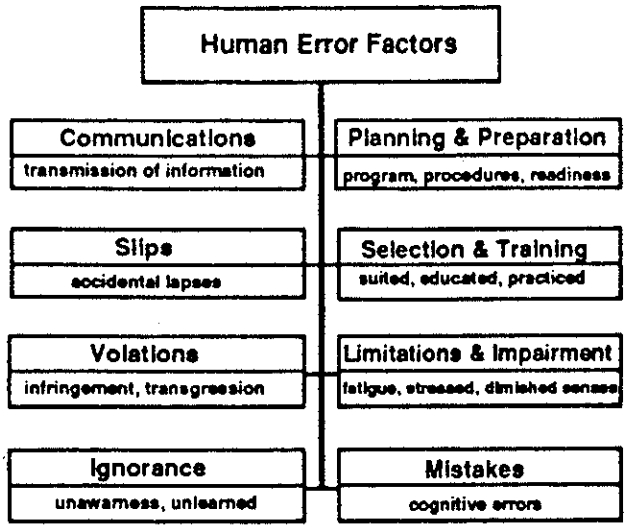


FIGURE 4. CLASSIFICATION OF HUMAN ERRORS

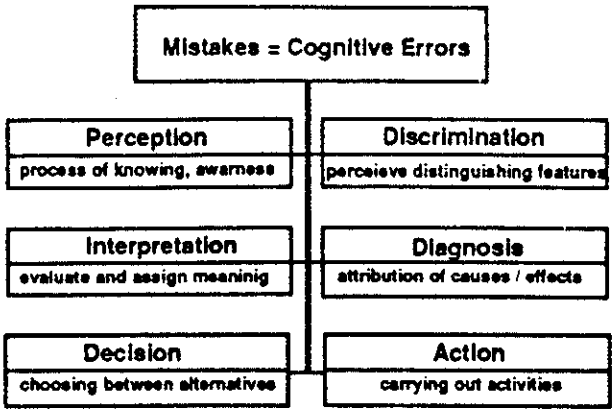


FIGURE 5. SOURCES OF MISTAKES

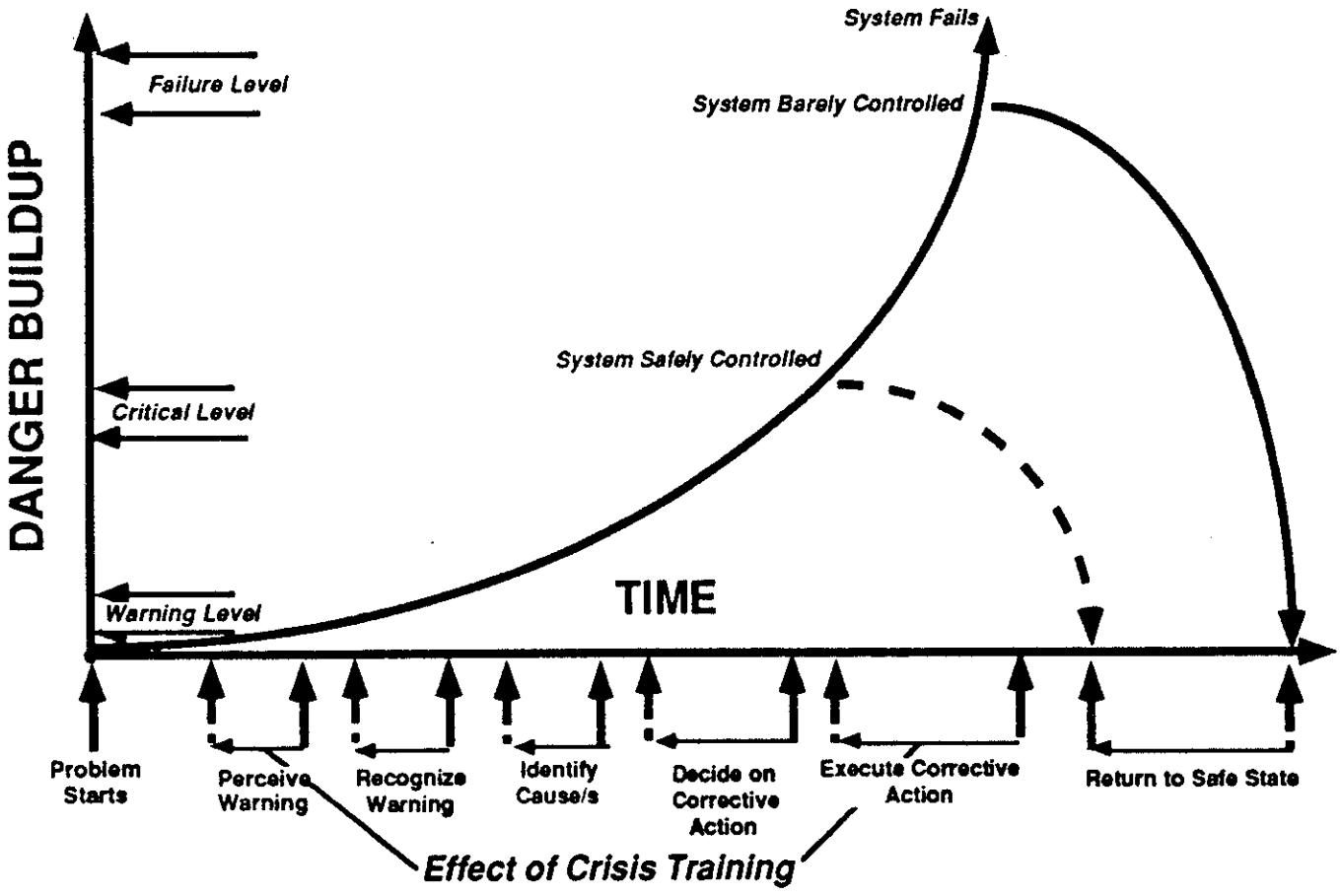


FIGURE 6. EFFECTS OF PERSONNEL SELECTION & TRAINING ON CRISIS MANAGEMENT

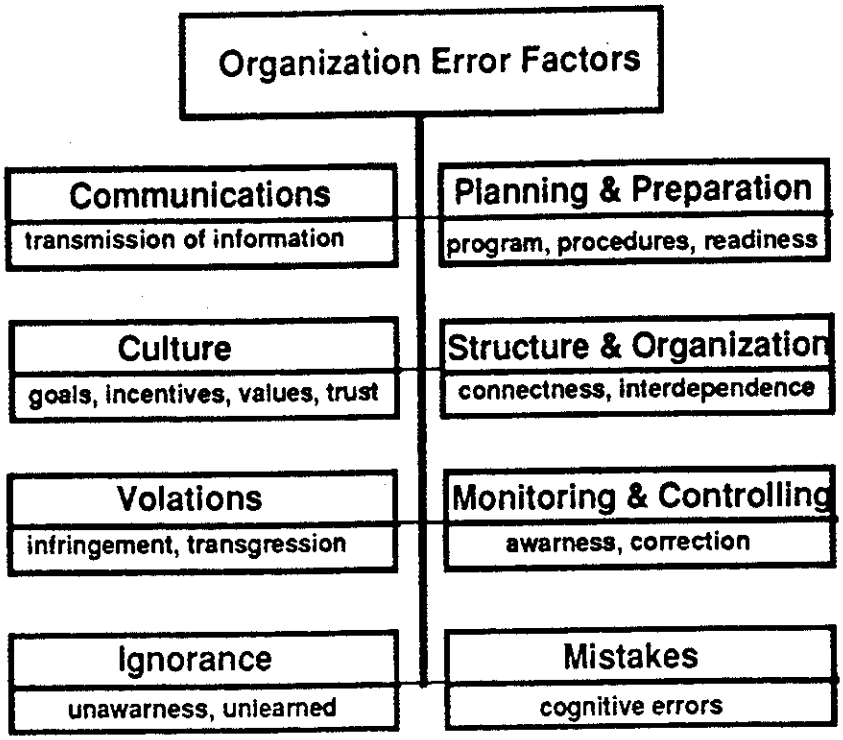


FIGURE 7. SOURCES OF ORGANIZATION ERRORS

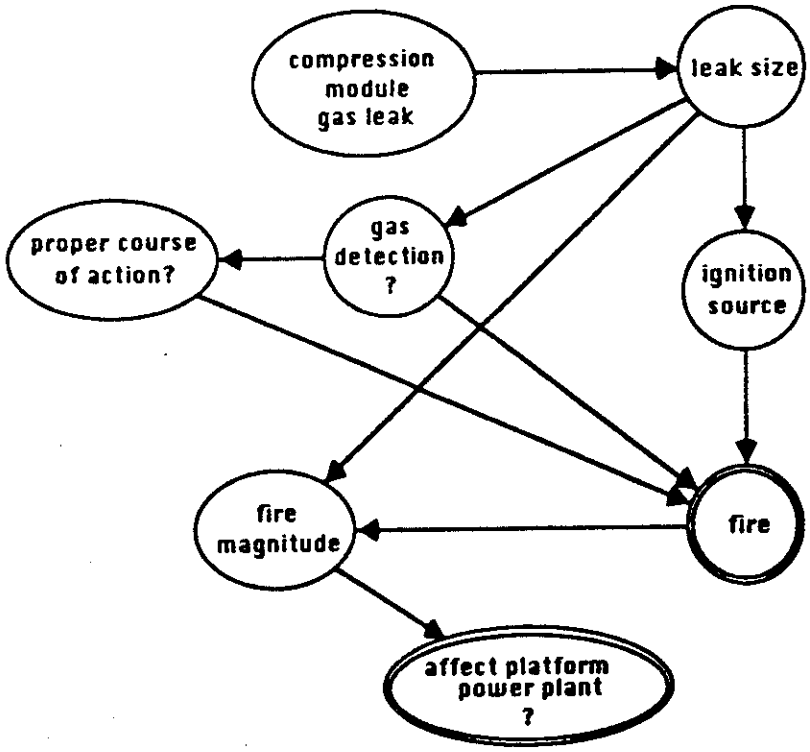


FIGURE 8. INFLUENCE DIAGRAM OF GAS LEAK IN PLATFORM COMPRESSOR MODULE